33

An Analysis of Network Management Traffic and Requirements In Wireless Networks

by

Pratip K. Banerji

Submitted to the Department of Electrical Engineering and Computer Science in partial fulfillment of the requirements for the degree of

Bachelor of Science in Electrical Engineering and Computer Science and Master of Engineering in Electrical Engineering and Computer Science

at the

Massachusetts Institute of Technology

May 23, 1997

Author .....
Department of Electrical Engineering and Computer Science
May 23, 1997

Certified by .....
Steven G. Finn
Thesis Supervisor

Accepted by .....
Arthur C. Smith
Chairman, Department Committee on Graduate Theses

An Analysis of Network Traffic and Requirements in Wireless Networks

by

Pratip K. Banerji

Submitted to the
Department of Electrical Engineering and Computer Science

May 23, 1997

In partial fulfillment of the requirements for the degree of Bachelor of Science in Electrical Engineering and Computer Science and Master of Engineering in Electrical Engineering and Computer Science

Abstract

Mobile wireless packet networks are becoming more common with the advances in the technology of digital communications, portable computers, and semiconductors. Network management in mobile wireless networks involves a variety of new issues not dealt with when managing immobile networks, and commonly used network management tools and protocols may not be ideal for a mobile environment. In this thesis, we show that the limited bandwidth of mobile wireless networks along with the need to monitor topology changes while keeping network management bandwidth usage at less than 5% may require alternative network management data gathering strategies on BBN Corporation's mobile wireless networks. Three alternatives to standard network management tools (SNMP) are discussed and analyzed for network bandwidth requirements, and a guide for choosing network management data gathering strategies on mobile wireless networks is proposed.

Thesis Supervisor: Dr. Steven G. Finn
Title: Principal Research Scientist, Laboratory for Information and Decision Systems

Acknowledgments

First off, I'd like to thank everyone at my 6A company, BBN Corporation, and in particular, Tony Michel and Mitch Tasman. With their guidance and support I have learned an immense amount, and without their support to the end, this thesis probably would not be completed. Also, many thanks to Dimitri Vlachos, Ted Haines, Franz Bronzo, and Bob Welsh for stimulating discussions as well as helping to make my time at BBN enjoyable.

Many thanks to Dr. Steven Finn. His uncountable hours of advice, proofreading, correcting, and rewriting have molded this thesis into what it is.

I'd like to thank my friends for their positive encouragement, concern, advice, late night zephyrs, coffee runs, and attempts to pleasantly distract me from the stress of thesis work.

Most importantly, I would like to thank my parents and my sister for their endless love, support, and encouragement all throughout my life. Without them, none of this would have been possible.

Table of Contents

Chapter 1

Background information

1.1 Introduction

Mobile wireless packet networks are becoming more common with the advances in the technology of digital communications, portable computers, and semiconductors. Network management in mobile wireless networks involves a variety of new issues not dealt with when managing immobile networks, and commonly used network management tools and protocols may not be ideal for a mobile environment. In this thesis, we show that the limited bandwidth of mobile wireless networks along with the need to monitor topology changes while keeping network management bandwidth usage at less than 5% may require alternative network management data gathering strategies on BBN Corporation's mobile wireless networks. Three alternatives to standard network management tools (SNMP) are discussed and analyzed for network bandwidth requirements, and a guide for choosing network management data gathering strategies on mobile wireless networks is proposed.

1.2 Mobile wireless packet data networks

Many different types of wireless networks exist (i.e. cellular telephony networks, satellite communications, etc.). This thesis focuses on mobile wireless packet data networks where packetized digital communication occurs between computers. Different strategies exist for routing of packets between computers in a mobile wireless networks. These strat-

egies range from using fixed based stations (similar to the routing used in cellular telephony), to ad hoc networks with peer-to-peer networking and clustering (Figure 1.1).

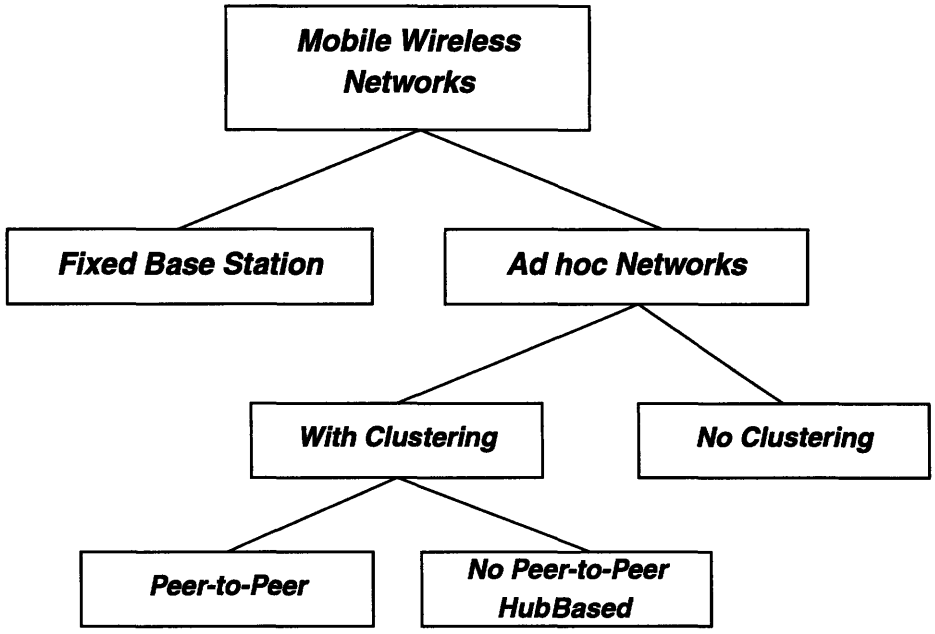

Figure 1.1: Types of wireless networks

The ensuing sections describe two major subsets of mobile wireless packet data networks: fixed base stations and ad hoc networks.

1.2.1 Fixed Base Station

The Internet Engineering Task Force (IETF) Mobile IP Working Group has been working to develop a standard for mobile communications over wireless networks [1]. The standard is based on a Fixed Base Station model, and relies on a static network infrastructure with mobile nodes connecting to stationary nodes (base stations). Each stationary node is responsible for radio communications with mobile nodes within its surrounding area. As a mobile node moves from cell to cell, the stationary node passes along the responsibility of handling the mobile node's packets. Ground based physical lines are used for communications between the stationary nodes. This type of wireless network is very

similar to the networking used in the cellular phone world, except that it does not rely on guaranteed bandwidth once a connection is open. A distinguishing characteristic of the IETF model is that it requires an existing static network infrastructure to function (Figure 1.2).

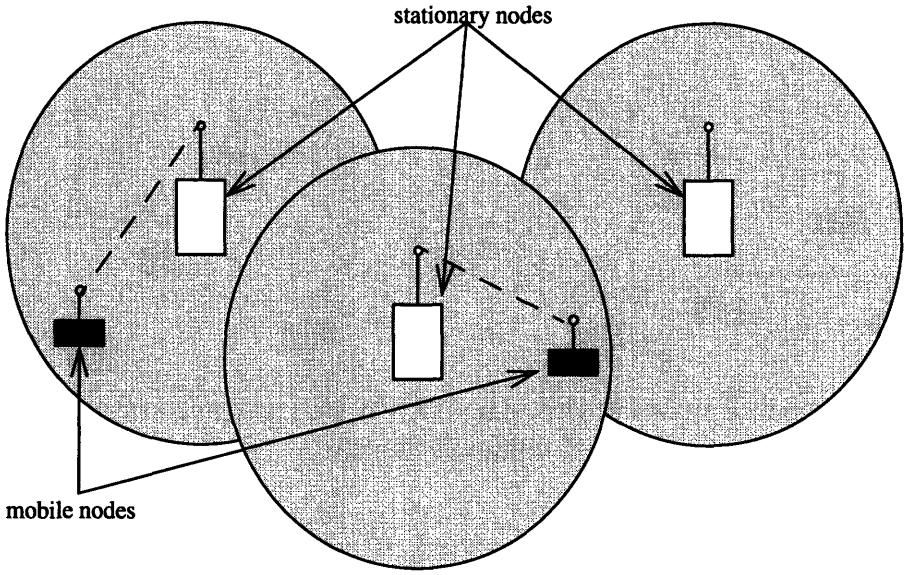

Figure 1.2: IETF model of wireless networking with three stationary nodes and two mobile nodes.

1.2.2 Ad Hoc Networks

At times, a fixed infrastructure may not be available for mobile nodes (or mobile hosts). For example, imagine a network formed in a battle area. Mobile hosts must form an *ad hoc network*, communicate *among* themselves as hosts, and *through* themselves to convey messages to other mobile hosts [1]. In essence, each mobile host is acting both as a switch (intermediate point), and a host (end point). The crucial difference between this and the IETF model of wireless networking is that there are no ground based physical lines between the intermediate points. In addition, the mobile hosts are mobile, so the entire topology of the network may be in constant transition.

Without clustering. Ad hoc mobile networks can be further divided into two types: those without clustering, and those with clustering. Without clustering, ad hoc networks operate strictly with peer-to-peer communications (Figure 1.3). There is no hierarchy, and each

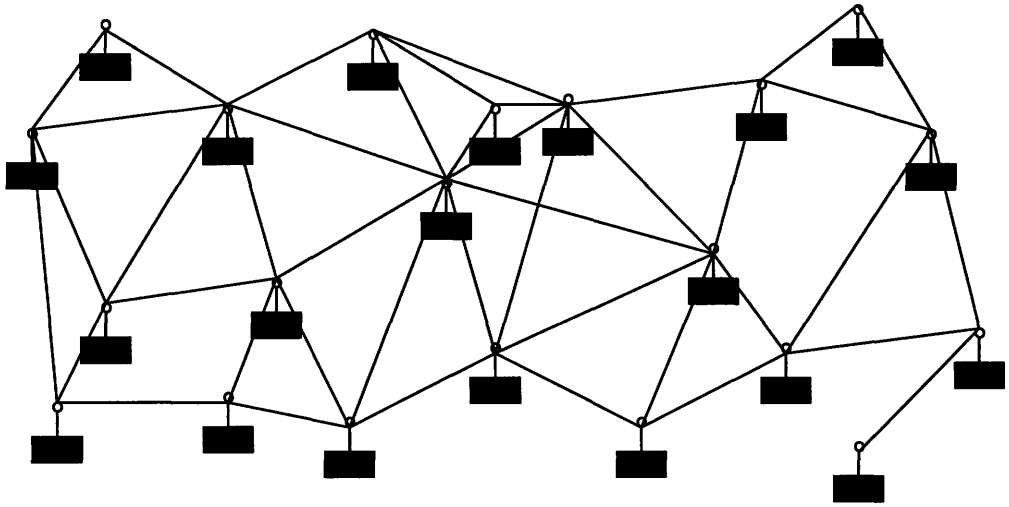

Figure 1.3: A mobile network with ad hoc networking and no clustering; peer-to-peer communications

mobile host acts as a router, forwarding packets as necessary. A mobile host needs to reconfigure its links when it either moves out of range of another mobile host that it has a communication link with or moves into the radio range of another mobile host. Such reconfigurations involve breaking a communication link and establishing a new communication link, respectively.

With clustering. Clustering provides a sort of subnetting (not at the IP level) by allowing a subset of mobile hosts to form their own sub network. One of the mobile hosts in each cluster is elected to be the *cluster head*, with the responsibility of communicating with other cluster heads. With clustering, the network is divided into two layers. The top layer is intercluster communication, and is carried out by the cluster heads. The bottom layer is intracluster communication, and involves messages passed between members of a cluster

(Figure 1.4). Clustered ad hoc networks without peer-to-peer communication require that

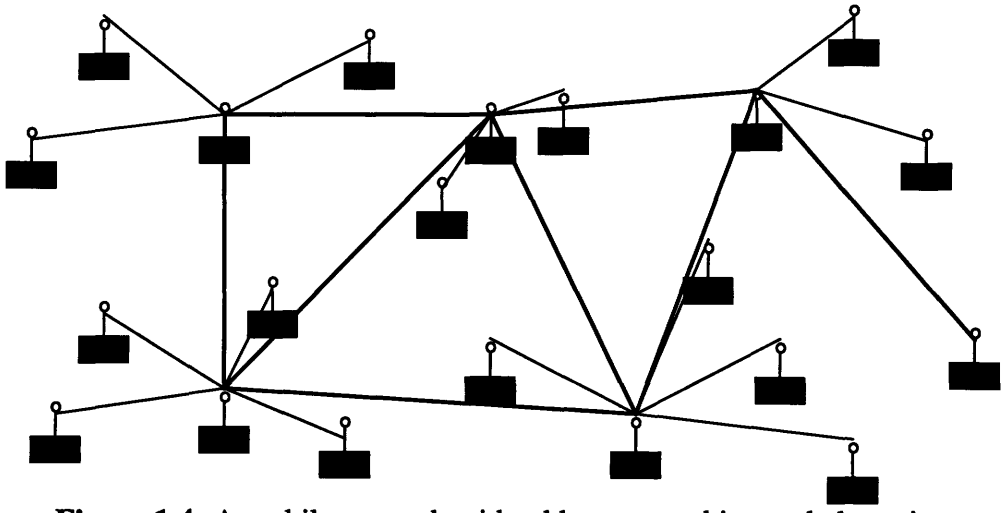

Figure 1.4: A mobile network with ad hoc networking and clustering

communication between mobile hosts within a cluster pass through the cluster head, whereas in a clustered ad hoc network with peer-to-peer communication, mobile hosts in the same cluster may communicate directly with each other. Although cluster heads have a promoted status and the extra responsibility of handling packets leaving the cluster, they still also act as mobile hosts.

The different methods for affiliating mobile hosts with clusters are not addressed in this thesis, but one potential method has each cluster head constantly transmitting a beacon. Each mobile host then constantly listens for beacons to ensure that the beacon with the strongest signal is the cluster head they are affiliated with. If it discovers a beacon from another cluster head is substantially stronger than the one from the cluster head it is affiliated with, it switches to the new cluster. If it finds that there are no cluster heads within range, it raises its power and becomes a cluster head.

1.3 The type of wireless networks considered in this research

The research described in this thesis focuses on ad hoc networks with no clustering. In addition to handling inter host routing, each mobile host must act as a router for a wireline local area network (LAN) connected to it.

1.4 Network management issues

Generally speaking, the network management process can be divided into two major components - the data display and processing (DDP) program and the data gathering and dissemination component. The DDP program is a high level network management application. This application is the primary interface between the network operator and the data gathering component. It generally provides a display map of the network topology, along with status indicators for each node. In most cases, this interface also provides some sort of alarm service. If there is a change in the network that the operator should be aware of, the DDP program is responsible for setting off an alarm that brings the change to the operator's attention. Also, the DDP program provides options and menus to help the operator with the network configuration process.

Underneath the DDP program lies the network management data gathering and dissemination component. This component acts as the broker between the network and the network operator's DDP program. Abstractly, it is responsible for populating the DDP program with data regarding the network topology, network node status, link status, traffic statistics, and other information that is needed from the network. It is also responsible for disseminating network management information to the network when needed. In many networks, tools such as SNMP [2] are used to obtain and distribute this information.

This thesis will focus the data gathering engine. We will develop information requirements for it, analyze its effectiveness and traffic load on the network, and propose alternate tools for use within the engine (Figure 1.5).

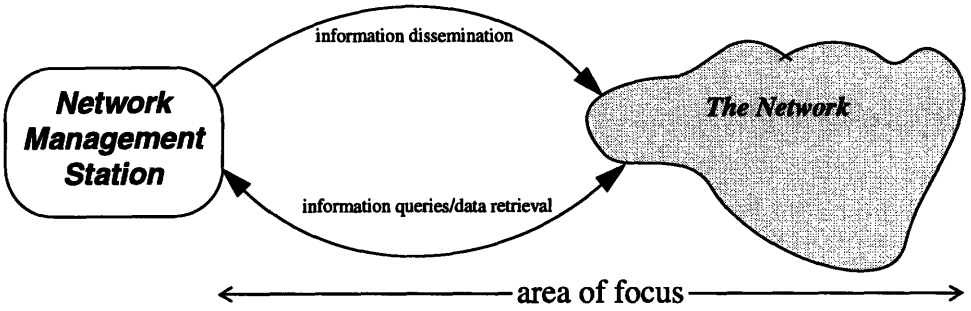

Figure 1.5: Our area of focus in network management

1.5 Current network management tools

For the purposes of data gathering and dissemination, network management applications use several different lower level tools to gather data and set configuration parameters. These tools are generally run by the DDP program, and they report their results back to the DDP program. Two commonly used low level tools for data gathering are SNMP and ping.

1.5.1 SNMP

SNMP is a protocol which defines two types of components - a *manager*, and *agents* [2].The manager is located on a host computer - typically one computer per network - and is responsible for polling the agents to request information. Agents run on each node of the network, collecting various information and storing it in an internal database. Agents return requested information to the manager when polled. SNMP's popularity stems from its simple design, ease of use, straightforward implementation, and expandability. It has become the industry's de facto standard, and almost all new networking products are built to support it.

SNMP provides various other functions including the capability to *set* as well as *get* parameters. It also allows for the setting of *traps,* or requests for the agent to notify the manager on some event triggering.

SNMP uses UDP for sending polls and receiving responses. SNMP packet format consists of a 20 byte IP header, an 8 byte UDP header, and a variable length ASN.1 encoded SNMP message [10].

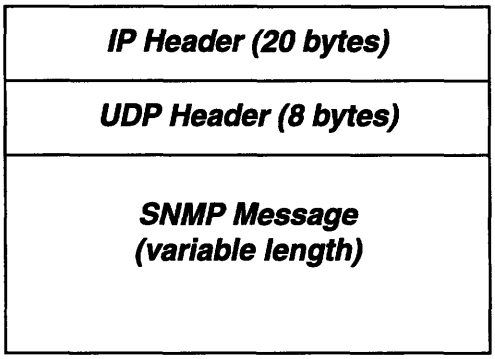

Figure 1.6: SNMP packet format

1.5.2 Ping

Another commonly used, but less revealing tool is the ping protocol. A ping is an ICMP echo request, which elicits an echo response from a host if the host is up [3]. A host's response to a ping poll indicates whether its network interface and operating system is working or not. Ping's small packet size make it a good tool for quickly assessing whether a host or router is up or down, but it provides no additional information.

1.5.3 Other network management data gathering tools

Other network management data gathering tools such as CMIP exist [4], but SNMP and ping are the most widely used industry tools. Our work primarily focuses on the use of the industry standard - SNMP.

1.6 Differences between mobile wireless networks and wireline networks

While SNMP and ping are today's most common network management data collection tools in wireline networks, it is not clear that these tools are appropriate in many mobile wireless networks because of important differences between the two types of networks. Two major differences between wireline and mobile wireless networks are that mobile wireless networks usually have less bandwidth between network nodes, and that the network topology of wireless mobile networks is changing frequently (as opposed to the almost constant topology of wireline networks).

1.6.1 Bandwidth limitations

Links between hosts in a mobile wireless network typically provide significantly less bandwidth than those in a wireline networks. Typical wireline network link bandwidths are between 1 Mbps and 100 Mbps, whereas typical mobile wireless links are between 1 kbps and 100 kbps [5]. With wireless bandwidths that are 3 to 5 orders of magnitude lower than that of a wireline network, network managers need to be more careful with traffic introduced on wireless networks than they are on wireline networks. Often, increases in power can offer higher link bandwidths on wireless networks, but mobility requirements often restrict the size and power of the battery source on mobile hosts.

Using SNMP and ping to poll for network management data may takes up considerable network bandwidth [7]. Although the individual packet sizes for SNMP messages are not by themselves overwhelmingly large, polling's constant retransmission of requests and responses consumes large amounts of bandwidth. An analysis of mobile wireless network bandwidth requirements for network management traffic will be developed in the thesis.

Differences between wireline and wireless link capacities may necessitate changes in or the replacement of the standard polling mechanisms of SNMP and pinging. It is not

clear when these changes will be required (what types of wireless network topologies and which bandwidth limitations), nor is it clear whether these polling tools can be modified to accommodate these changes. We investigate and quantify these limitations for different network topologies, and propose alternatives to SNMP and ping polling.

1.6.2 Dynamically changing network topologies

Typical network management tools aren't built to deal with the dynamic changing topology of ad hoc wireless networks. Links on conventional networks may occasionally go up and down, and the amount of traffic flowing on a particular link may change, but changes in topology are uncommon. In addition, nodes are usually stationary in location and connectivity. Even in a cellular network with fixed base stations, there is movement of the phone user within a cell and between cells, but the position of the cell's base station remains fixed.

For the network management tool to follow topology changes as well as node status changes of mobile hosts, it must poll at least once each time the topology changes. If topology has the potential to change rapidly, then the network management tool must poll frequently to discern the changes. Picking a constant polling rate may be inefficient when the rate at which topology is changing is not constant. We will also explore adaptive polling rates in this thesis.

1.7 Problem statement and network model

This work was originally started at BBN Corporation as a project to optimize the use of network bandwidth by network management traffic in BBN multihop packet radios. BBN has been researching multihop packet radios since the late 1970s [6], and in recent years has been applying variations of this technology to numerous research, commercial, and military networks. The variation of the multihop packet radio that we are studying is a

mobile wireless network that uses ad hoc peer to peer networking without clustering.

1.7.1 Network management on the BBN network

We are interested in investigating whether standard SNMP polling mechanisms can be used to monitor BBN's mobile wireless network. Specifically, bandwidth over the wireless links between the mobile hosts is limited, and SNMP's polling intensive nature can introduce large amounts of network management traffic on these links [7]. BBN requires that network management traffic not exceed 5% of the overall network bandwidth. In other words, 95% of each network link's bandwidth should be available for user and other system traffic. Standard SNMP polling may not meet this restriction as the number of mobile hosts in the network increases.

1.7.2 BBN network model and information requirements

Two sets of parameters are used throughout this thesis in analyzing network management traffic: network parameters and information model parameters. After accounting for link setup, maintenance, and tear down overhead, each mobile host has approximately 400 kbps is available for data transmission. In our analysis, we will assume a grid topology,

with each mobile host connected to a maximum of four other mobile hosts (Figure 1.7). With half duplex links, this allows for a 50 kbps link rate over each link in each direction.

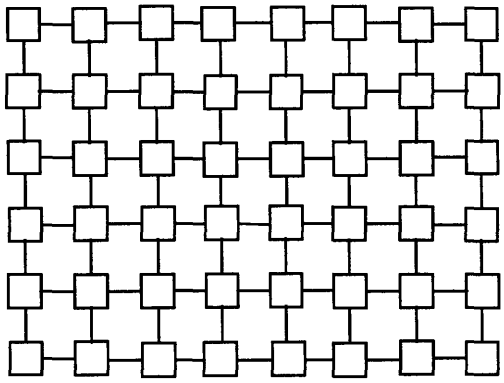

Figure 1.7: Typical BBN mobile wireless network topology

BBN also has certain network management information requirements - high priority fault detection within 30 seconds, low priority fault detection within 5 minutes, topology change detection within 60 seconds, and performance management updates at 1800 second intervals (these terms are explained in detail in Chapter 2). The specific quantity of data (number of SNMP polls and responses, and the size of their packets) required by BBN to stay within these requirements will be discussed in Chapter 2.

1.8 Thesis goal

We will explore the suitability of SNMP for collection of network management information in BBN's mobile wireless network, consider possible alternatives, and examine their efficiency.

1.8.1 Motivation

With limited bandwidth provisions over BBN's mobile wireless network links, and an increasing number of mobile hosts to monitor, it is not clear that current network management technologies and tools are adequate to maintain sufficient and timely network status

information while maintaining a bound on the percentage of network management traffic on the network.

Under conditions with a small number of mobile hosts, a long polling interval, and high bandwidth links, SNMP tools may provide adequate and timely network management data for BBN's mobile wireless network. With a larger number of mobile hosts, the number of poll requests that must be made to adequately monitor the network increases. With that, the amount of network management traffic generated by the network management tool increases, and a large amount of traffic must be transmitted over the links of the mobile host adjacent to the network management tool. Similarly, networks with lower link bandwidth capacity, or network management requirements for more timely responses to network status changes (requiring a higher polling rate) lead to a higher percentage of network management traffic on a network.

1.8.2 Alternatives to standard network management

Several alternatives exist to the current network management SNMP based tools. In this work we will focus on three alternatives that reduce network management data gathering bandwidth requirements. Each of these alternatives uses a different mechanism for lowering the amount of bandwidth generated by network management traffic, but with each of these solutions comes certain tradeoffs. The tradeoffs include implementation man hours, modularity of network management system, ease of transition of network management method to new technology networks (new routing algorithms, different media, etc.), timeliness of response to active polls, and the time taken for the network management tool to realize a status change in the network.

The first, and perhaps most simple to implement, strategy is an adaptive SNMP polling algorithm. Only the network management station's (NMS) client program needs to be

modified to perform this task, but with its simplicity comes a reliance on an upper bound on network mobility.

The second strategy is to have mobile hosts proxying network management responses for groups of mobile hosts. Major software modifications of the network management program on the mobile hosts and the NMS are required for this strategy. In addition, it may take longer to get information because information must be staged first in the proxy server mobile host.

The third strategy is to use a network management method which reads Open Shortest Path First (OSPF) routing updates to provide network status information. This method can replace a significant amount of network management traffic but cannot replace all the information required by the data display and processing program on the NMS. In addition, this requires writing additional software on the network management tool.

Each of these methods is discussed in detail in Chapter 4.

1.8.3 Thesis goal and organization

The broad goal of this thesis is to provide a guide for network architects and planners of network management systems to use in determining which type of network management data collection techniques are suitable for mobile wireless networks. The assumptions, models, and final presentation of results is based on BBN's specific mobile wireless network, but the parametrized model should be of use to different wireless network situations.

The second chapter of this thesis is devoted to developing the network management information model requirements for mobile wireless networks. It begins by defining general network management goals, and then moves on to describing how these goals compare to wireline network management goals. In the process, it also defines different types

of faults, configuration management issues, and how much performance management needs to be done. It concludes with a traffic model for BBN's mobile wireless network's network management traffic requirements.

The third chapter identifies two representative mobile wireless network topologies and develops analytical techniques for calculating the link bandwidth required to support the network management system's data collection traffic as defined by the information model. These techniques calculate link bandwidth requirements as a function of the topology, message sizes, number of nodes, and polling rates.

In the fourth chapter we describe the three proposed alternative strategies to standard SNMP for network management data collection in a wireless network and analyze their bandwidth requirements. The fifth chapter draws conclusions and proposes some guidelines for which strategy is appropriate for a mobile wireless network as a function of BBN's available link rate, and network management information requirements. The sixth chapter provides a conclusion.

Chapter 2

Information model for wireless network management

2.1 Introduction

In this chapter we introduce general network management goals for wireless networks, show how mobile wireless networks differ from wireline networks, and develop a parametrized information model for estimating network management data gathering bandwidth requirements.

2.2 General network management goals

Network management's twin goals are to reduce the number of network problems, and minimize inconvenience and contain damage when problems occur. To achieve these goals the Internet Standards Organization (ISO) has defined five network management functional areas. These five areas are fault management, configuration management, performance management, security management, and accounting management [8].

1. Fault management

The facilities that enable the detection, isolation, and correction of abnormal operation of the Open Systems Interconnection environment[1].

2. Performance management

The facilities needed to evaluate the behavior of managed devices and the effectiveness of communications activities.

3. Configuration management

1. The Open Systems Interconnection reference model describes network protocols, and was devised by the ISO.

The facilities that exercise control over, identify, collect data from, and provide data to managed devices for the purpose of assisting in providing for continuous operation of interconnection services.

4. Security management

Addresses those aspects of OSI security essential to operate OSI network management correctly and to protect managed devices. There are two aspects of security management. The first is the management of the security of a network, and the latter is the security of the management aspects of the network. To contrast, one involves monitoring whether a given network is secure, while the latter is composed of ensuring the security of the network management process.

5. Accounting management

The facilities that enable charges to be established and costs to be identified for the use of managed devices.

In this thesis we focus on the first two areas of network management: fault management and performance management. We do this because these two dominate the bandwidth and timeliness issues of network management.

Normally, transmission of data through radio is considered insecure, but in our case, we will assume that the wireless hosts use secure transmissions at the physical layer (e.g. cryptography). In other words, anything that is transmitted over the air is assumed transmitted securely, so the network management layer does not need to worry about that aspect of the network.

Generally speaking, accounting is difficult in ad hoc wireless networks. Everyone's radio acts as a common resource for other radios to route packets through, and it is difficult to track actual packet flow per user. For the purposes of this thesis, we will disregard billing and accounting.

Although configuration management is a vital part of the network management model, there are a variety of reasons for not including it within our analysis of bandwidth usage. Configuration changes occur at random intervals on random hosts within the network. Configuration changes do not occur often, and most mobile host configuration is done before network deployment. Hence, the actual bandwidth consumed by configuration changes is both unpredictable and small compared to the total network management traffic.

2.3 Fault and performance management in mobile wireless networks

2.3.1 Fault management

With respect to network management, our first and foremost concern is to be aware of faults in the network, and correct them, if possible, when they occur. Generally speaking, a fault refers to a problem that can cause a network to not function as planned. Specifically, the ISO defines fault management to consist of the facilities that enable the detection, isolation, and correction of abnormal operation of the ISO environment [10].

To facilitate our information model requirements, we will break network faults into two categories: high priority network faults, and low priority network faults. The first is a fault that results in a mobile host being completely inoperational or unreachable. In this case the mobile host will not respond to any network queries, including SNMP or ping requests. Furthermore, it will be unable to perform in its role of forwarding packets. Typical causes of this in a wireless network can be a mobile host equipment failure or loss of connectivity to the rest of the network due to its drifting out of radio range.

The second type of fault, a low priority fault, is one that doesn't completely incapacitate the mobile host, but leaves a small portion of the network dysfunctional or unreach-

able. An example of this would be a mobile host which is able to communicate with other mobile hosts, but for some reason, cannot communicate with its local users.

High priority network fault. What makes a high priority network fault high priority? BBN's mobile hosts have multiple network interfaces, with the primary interface being the wireless interface, and the secondary interfaces being wireline connections to local users. The wireless interfaces construct the primary backbones for end-to-end communication between the devices on the wireline network. The physically wireline interfaces provide connectivity for the users actually involved in end-to-end communication. Any network fault that has the potential to affect more than the local users connected to a mobile host is considered a high priority fault.

The consequent network-wide problems that high priority network faults can cause requires that we poll for high priority network faults frequently. We define the high priority fault polling interval (in seconds between polls) as PI_{hpf}, and the length of a high priority poll and its response as LP_{hpf} and LR_{hpf}, respectively.

Low priority network fault. A low priority network fault is one that does not affect the overall network performance, but rather, a small subset of the network. More concisely, faults involving other local area network interfaces hanging off each mobile host qualify as low priority faults. For example, one of the local interfaces could fail, or one of the local terminals could fail.

Due to the isolated effects of each of these outages, low priority faults need not be monitored by the network management tool at the same frequency as that of high priority network faults. We define the low priority polling interval (in seconds between polls) as PI_{lpf}, and the length of a low priority poll request and its responses as LP_{lpf} and LR_{lpf}, respectively.

2.3.2 Performance management

Monitoring network performance is a critical aspect of network management. Current network performance in conjunction with performance history can be used to predict failures before they occur. Unlike fault management, which is reactive process of learning when network faults occur, and then correcting them, performance management needs to be a proactive process. The performance of the network needs to be frequently monitored to understand traffic usage patterns and where network bottlenecks exist, etc. Network performance monitoring is a heavy user of network bandwidth.

Performance management can detect problems such as congestion (too much traffic flowing through one mobile host, resulting in large packet queues and delays). Congestion is prone to occur in networks with bottlenecks and coupled with moderate to high traffic flow, it can lead to high or low priority faults in a network.

An example of a network bottleneck can be seen in Figure 2.1. By watching topology changes we can actually predict when a mobile host fault may lead to the isolation of a portion of our network, and correct it before a fault occurs (perhaps, if possible, by having

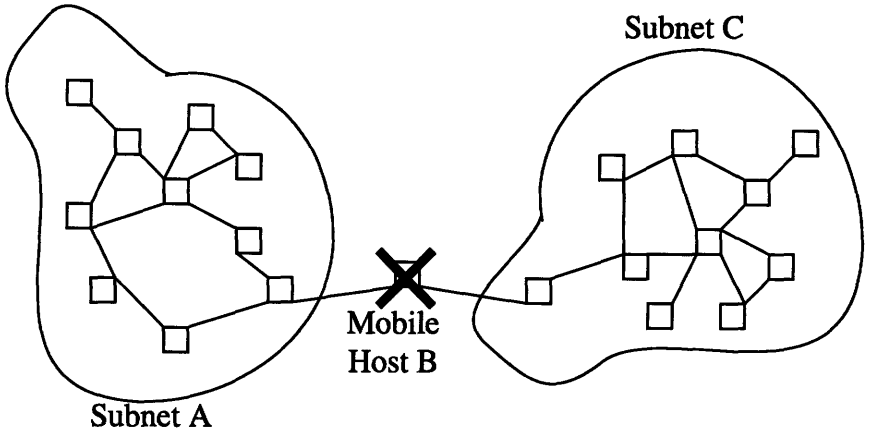

Figure 2.1: A network becomes disjoint due to a bottleneck condition

another mobile host move in between the two almost-disjoint networks the provide another redundant path).

Because mobile wireless mobile networks have topologies that are more dynamic than wireline networks, topology detection needs to occur more frequently than other performance detection tasks. Therefore, we feel it is rational to separate performance management into two parts - topology monitoring, and the rest of performance management. The former should be monitored frequently, and the latter need not be followed as closely. We will refer to the polling interval of topology monitoring (in seconds) as PI_{tm}, and the length of the poll and its response (in bytes) as LP_{tm}, and LR_{tm}, respectively.

We feel that the rest of performance management is similar in timeliness requirements to low priority fault detection timeliness requirements. Variables on a mobile host such has packets in/packets out, CPU load, etc., should be monitored as frequently as low priority faults. We use PI_{pm} to denote the polling period for performance management (exclusive of topology management), and LP_{pm} and LR_{pm} to denote the length of a performance management poll and its response.

In Table 2.1 we provide a summary of the different poll types, their respective polling intervals and poll/request lengths, and a brief description of their functions.

Poll type	Polling interval	Length of poll (bytes)	Length of response (bytes)	Description
High priority fault detection	PI_{hpf}	LP_{hpf}	LR_{hpf}	Detecting high priority faults. e.g. a mobile host failure.
Low priority fault detection	PI_{lpf}	LP_{lpf}	LR_{lpf}	Detecting low priority faults. e.g. a mobile host's interface to its LAN is down.
Topology management	PI_{tm}	LP_{tm}	LR_{tm}	Following topology changes in network. e.g. a mobile host has drifted out of range from one mobile host, and is communicating through another.

Table 2.1: Data collected from network

Poll type	Polling interval	Length of poll (bytes)	Length of response (bytes)	Description
Performance management	PI_{pm}	LP_{pm}	LR_{pm}	Data gathering of performance characteristics of network. e.g. a mobile host is overloaded by too much traffic and is dropping packets.

Table 2.1: Data collected from network

Chapter 3

Network models

3.1 Introduction

In this section, the characteristics of BBN's mobile wireless networks are identified. Using that as a base, the bandwidth consumed by the network management traffic is analyzed for polling mobile hosts for two different wireless network topologies, different bandwidth limitations, and topology change notification requirements. We will determine the link bandwidth at which the network limit network management traffic is less than 5% of overall network traffic capacity over each link.

3.2 Characteristics of mobile wireless networks

3.2.1 Communication link performance

Performance characteristics of a network link are often expressed in terms of link rate and propagation delay. Link rate is the rate (in bits per second) at which data can be sent over a link at a certain bit error rate. The propagation delay refers to the time elapsed between a bit of data entering the network link at the source mobile host and it leaving the network link at the destination mobile host.

The SNMP packets we are sending are more than 32 bytes (UDP/IP packets are a minimum of 32 bytes for headers alone) [11], or 256 bits. Assuming we have a 100 kbps link, it would take a minimum of 2.56 milliseconds to transmit this packet on to the link. Mobile hosts are typically within a few miles of each other (1 to 5 miles, or 1.5 to 8 km), and rate of propagation is the speed of light ($3x10^8$ m/s). Hence, the propagation time for two mobile hosts that are 8 km apart is 0.025 milliseconds. The ratio of the propagation time to the transmission time is approximately $1x10^{-2}$ (Equation 3.1).

$$\frac{\text{propagation time}}{\text{transmission time}} = \frac{0.025}{2.56} \approx 10^{-2} \tag{3.1}$$

Therefore, for the purposes of this analysis, we consider propagation delays to be insignificant compared to transmission times (linearly related to link rate). We disregard propagation delays, and focus solely on link rate.

As stated in Chapter 1, BBN's mobile wireless network has link rates of 50 kbps per second in each direction. For this analysis, we will leave the link rate as a variable parameter so as to allow this analysis to be reapplied if BBN improves their network's link rate.

3.2.2 Mobility (topology changes)

One crucial factor differentiating mobile wireless networks from wireline networks is that the topology may be constantly changing. When referring to topology change, we are not explicitly discussing a mobile host changing its geographical location by moving around on the field, but rather, a movement that causes a change in the node to node topology. For example, a mobile host can establish a link with another mobile host who it moves closer to, while losing a link with a mobile host that it was once linked to.

For high mobility networks, the topology polling interval, PI_{tm}, needs to be short. For networks that are not as dynamic, a larger polling interval can be used.

3.2.3 Network structure

In analyzing BBN's dynamic mobile wireless networks, there are too many possible network topologies for one to consider all. We chose to analyze variants of 2 network structures that we believe offer a reasonable representation of typical mobile wireless network topologies. These network structures have a maximum of four links connecting any mobile host to another mobile host. In reality, the number of links between mobile hosts is dictated by the location of each mobile host, the number of radio frequencies or interfaces

available for communication, and by the range of its radio signal. A consideration for future work is a more rigorous analysis of statistics gathered by observing mobile wireless networks in use.

The two different topologies that will be analyzed:

1. Uniform distribution ($\sqrt{N} \times \sqrt{N}$ grid)

2. Elongated distribution ($\frac{\sqrt{N}}{\alpha} \times \alpha\sqrt{N}$ grid, with $\alpha>1$)

These two topologies will be considered in more detailed in section Section 3.4.

Network characteristics	Description
Communication link performance	Link rate - the rate at which data can be sent over a link.
Mobility	A movement that causes a change in the node to node topology of the network
Network structure	The node to node topology of the network

Table 3.1: Summary of network characteristics and descriptions

3.3 Network bandwidth usage

To understand network management bandwidth requirements, we must first determine the amount of data that must flow across each network link over a period of time.

High priority network fault detection, as described in Chapter 2, must occur frequently. BBN requires high priority fault detection within 30 seconds, so we choose the high priority polling interval (PI_{hpf}) as 30 seconds. SNMP uses UDP to send messages with ASN.1 encoding (no fixed fields) [11]. The size of the SNMP poll requests are approximately 73 bytes (20 bytes for the IP header, 8 bytes for the UDP headers, and a varying size for the SNMP message, with the typical size being 45 bytes). Each mobile host needs to be polled once every 30 seconds, so within each polling period there is one

high priority fault poll of 73 bytes (LP_{hpf}). SNMP responses have the same header information, but the actual data in the SNMP message can vary considerably. We assume the size of a simple SNMP response for high priority fault information is also 73 bytes (LPR_{hpf}).

Low priority network faults need to be monitored less frequently. To meet BBN's requirement of detecting low priority faults within 5 minutes, we set the low priority polling interval, PI_{lpf}, at 5 minutes (300 seconds) [12]. Each of BBN's mobile hosts has four external interfaces that need to be monitored for low priority network faults. We need to send one SNMP poll for each interface. The total length of the polls per mobile host is approximately 292 bytes ($73 \text{ bytes} \cdot 4 \text{ interfaces}$). The size of the SNMP responses to these polls is also approximately 292 bytes.

Because wireline networks generally have static network topologies, no standard SNMP variable exists for storing topology information. One possible method for deducing network topology is to use SNMP to retrieve the routing tables of mobile host. This method may not always return complete results, and in the case of mobile wireless ad hoc networks, each mobile host needs to have a route to every other mobile host. Hence, the size of the routing tables returned is large (increasing linearly with N, the number of mobile hosts). BBN feels a better way to monitor topology on wireless networks is to have the mobile host store an SNMP table variable in the management information base (MIB) with the list of mobile hosts it is connected to. To request the entries in this table, the SNMP polling client first requests the first entry in the mobile host's mobile host connection status table, followed by the second, and continues until all the connection information has been collected. The size of the polls and responses are constant, and the number of polls and responses is linearly related to the number of connections to mobile hosts. The size of an SNMP poll is approximately 73 bytes, and one response is approximately

77 bytes. For our model, we are assuming that on the average, each mobile host is connected to four other mobile hosts, so there are a total of four polls and four responses. Hence, a total of 292 bytes are sent in polls, and 308 bytes in responses. BBN requires topology detection within 60 seconds, so the polling interval for topology management (PI_{tm}) is 60 seconds [12].

Numerous performance monitoring MIB variables exist, and it is up to the network architect and network management planner to decide which variables need to be monitored. BBN requirements state that the network management station needs to monitor approximately 10 MIB variables per mobile host to monitor performance. Each poll, once again, requires 73 bytes. For the variables required from BBN's mobile hosts, each response requires an average of 80 bytes. Generally, performance management polling intervals are high, and in practice, are sometimes not even gathered at periodic intervals. BBN requires performance management updates at 30 minute intervals, so we choose a polling interval for performance management (PIpm) of 30 minutes (1800 seconds).

Poll type	Poll interval (PI)	Total length of polls (LP)	Total length of poll responses (LR)
High priority fault (hpf)	30 seconds	73 bytes	73 bytes
Low priority fault (lpf)	300 seconds	292 bytes	292 bytes
Topology monitoring (tm)	60 seconds	292 bytes	308 bytes
Performance management (pm)	1800 seconds	730 bytes	800 bytes

Table 3.2: Polling interval and length of poll of different poll types per mobile host

The links on BBN's mobile wireless network provide for duplexed communications, hence half of the total bandwidth is used for traffic in each direction. BBN's OSPF routing

algorithm always provides the shortest path between the NMS and polled node, so given any link we know that network management polling traffic is guaranteed to flow in only one direction, and the responses are guaranteed to flow in the other. Hence, because the lengths of the responses are larger than the polls, to maintain the 5% cap on network management traffic we only need to analyze the traffic generated by the responses.

The total NMS bandwidth required by the responses for one mobile host is:

$$BW^{R}_{SNMP} = \left(8\frac{bits}{bytes}\sum_{hpf,lpf,tm,pm}\frac{LRx}{PIx}\right)bps \tag{3.2}$$

Every packet takes the shortest path from the NMS to the mobile host it is polling, so we can determine the expected traffic on any link over a given period of time. To determine the bandwidth used by the response traffic in any polling cycle:

1. For each mobile host we are polling, we need to:
   - Determine all possible shortest paths between the NMS and the mobile host.
   - For each possible link traversed, determine the probability of traversing that link while polling this mobile host (the number of paths crossing this link divided by the number of total paths between the NMS and the mobile host); multiply that probability by the sum of the size of the poll response.
   - Store the value as the bandwidth used on that link for one poll to that mobile host.
2. Do this for all routers that we are polling in one polling cycle.
3. For each link, sum together the bandwidth values stored from each poll.

We would then have the expected total bandwidth used for SNMP responses on each link per polling cycle.

3.4 Typical network scenarios

Here we will discuss different network scenarios typical of our networks, and provide a general mathematical analysis of them.

3.4.1 A uniform network distribution

The first topology is a uniform network distribution. Each mobile host has four links connecting to its neighbor mobile hosts, except for edge mobile hosts which have three links each, and corner mobile hosts which have two links each (Figure 3.1).

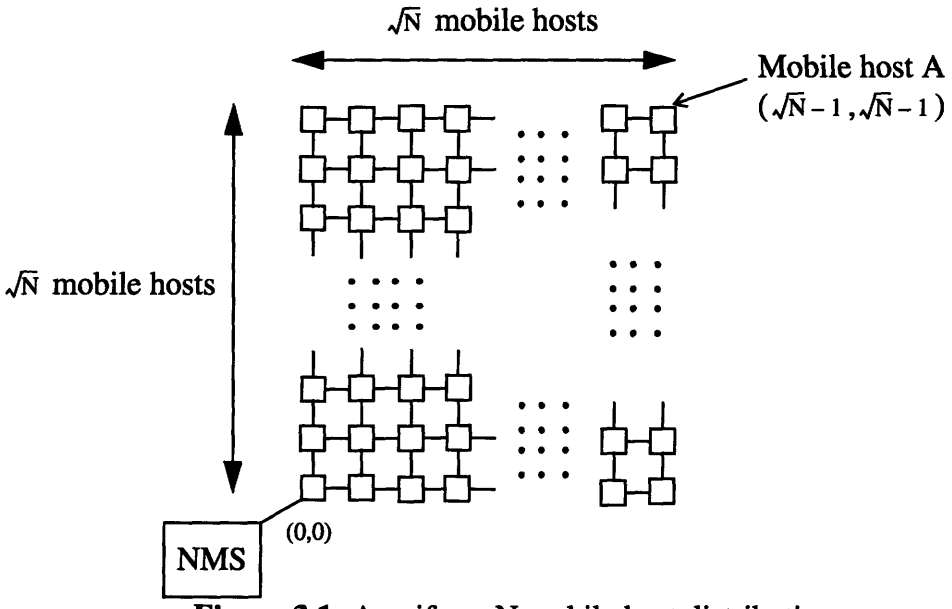

Figure 3.1: A uniform N mobile host distribution

As stated in the Chapter 2, in wireless network management we are primarily concerned with network management traffic for fault management and performance management.

The analysis of periodic polling protocols is fairly well established [13]. With one SNMP network management entity polling multiple devices (mobile hosts) every T sec-

onds, with Δ being the minimum time required to complete one poll, the number of mobile hosts that can be managed with serial polling is:

$$N \leq \frac{T}{\Delta} \tag{3.3}$$

The components of Δ include:

1. The time it takes to package the message on the network management tool (processing time).
2. The time it takes to output the message on the radio link (transmission time).
3. The network latency from the network management tool to the polled client (propagation time).
4. The time taken for the polled client to interpret and process the SNMP request (processing time).
5. The time it takes for the polled client to package the response (processing time).
6. The time it takes to output the message on the radio link (transmission time).
7. The network latency from the polled client to the network management tool (propagation time).
8. The time taken for the network management tool to process the request (processing time).

Looking at the transmission time alone, we find that to poll a uniformly distributed network of N nodes, we need to send an SNMP poll every T seconds to each of the N nodes. Each SNMP poll and its response is at least 60 bytes. With 50 kbps links, the transmission time for each node to forward an SNMP poll packet is:

$$\text{Transmission time per node for SNMP polls} = \frac{60 \text{ bytes} \cdot 8\frac{\text{bits}}{\text{byte}}}{50,000 \text{ bps}} = 9.6 \text{ milliseconds} \tag{3.4}$$

In a uniformly distributed network of N nodes, an average of $\sqrt{N}$-1 links need to be traversed for each poll, and the same number of links need to be traversed when the

response returns. Hence, on the average, the minimum transmission delay per poll and response are:

$$\text{Delay per poll}_{\text{transmission}} = (\sqrt{N} - 1) \cdot 2 \cdot 9.6 \text{ milliseconds} \quad (3.5)$$

In a relatively small network with 200 nodes, the average delay resulting from transmission times is:

$$\text{Time to poll 200 node network} = 200 \cdot \text{Delay per poll}_{\text{transmission}} = 50.4 \text{ seconds} \quad (3.6)$$

So, if we assume that we have no queueing, propagation, or processing delays, it takes 50.4 seconds to poll 200 nodes in one polling cycle for high priority faults alone. The packet sizes of the responses to low priority fault polls, topology management polls, and performance management polls are larger, and produce larger delays. If the polling interval is not longer than the time it takes to cycle through polling all the nodes, the network's nodes cannot be monitored using the technique described above. The key problem in this polling mechanism is the fact that the network management tool has one client process that executes a poll and blocks until a reply is returned (i.e. serial polling).

To overcome this problem, network management tools typically start multiple threads which concurrently poll routers on the network (i.e. parallel polling).

Analysis strategy. Instead of evaluating all the paths between the source host (the NMS) and the destination host (the mobile host being polled), and then, for each link, counting the number of paths that crossed it, the number of paths crossing a particular link can be represented as the product of the number of paths between it and the source, and the number of paths between it and the destination.

For example, assume we are trying to find the expected network management traffic over one link from one poll of a node on a $\sqrt{N} \times \sqrt{N}$ network such as the one shown in

Figure 3.1. With the bottom left node with the NMS labeled (0,0) and the top right node labeled ($\sqrt{N}$-1,$\sqrt{N}$-1), assume we are polling node (m,n) (with $m \leq \sqrt{N} - 1$ and $n \leq \sqrt{N} - 1$), and are looking for the traffic over the link between (p,q) and (p,q+1) (with $p \leq m$ and $q + 1 \leq n$). The number of paths between (0,0) and (p,q) can be given by the combinatoric function:

$$\binom{p+q}{p} = \frac{(p+q)!}{(p+q-p)!p!} = \frac{(p+q)!}{p!q!} \tag{3.7}$$

This can be derived through the following process. First of all, assume we are trying to find the number of shortest lattice path from (0,0) to (r,s), where r and s are nonnegative integers. Each of these paths can be decomposed into horizontal and vertical moves of the respective forms:

$$(x,y) \longrightarrow (x+1,y) \text{ and } (x,y) \longrightarrow (x,y+1)$$

Any given shortest path between (0,0) and (r,s) will clearly have r+s moves, and any sequence of these moves must be some combination of r horizontal and s vertical moves. Therefore, counting the paths between (0,0) and (r,s) is equivalent to counting the number of sequences of moves.

So, essentially, the problem is one of how many sequences of r+s symbols are there, where r or them are "H" (horizontal) and s of them are "V" (vertical). To solve this problem, envision r+s empty slots, and count the number of ways you can fill r of them with "H"s, with the remainder filled with "V"s. The number of size r subsets (the slots with "H"s) of a set r+s elements (the total number of slots), is equal to "(r+s) choose r", or the binomial expansion of (r+s,r), or:

$$\binom{r+s}{r} = \frac{(r+s)!}{(r+s-r)!r!} = \frac{(r+s)!}{r!s!} \tag{3.8}$$

This can easily be seen if we look at a simple 3x3 network (Figure 3.2).

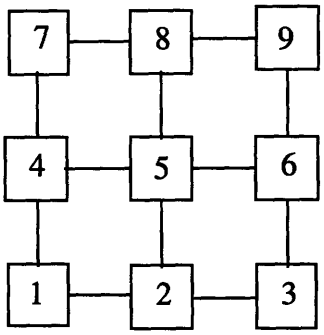

Figure 3.2: A simple 3x3 grid network

The shortest path from 1 to 9 is 4 hops, and by simply counting the paths, it is clear that there are 6 paths between the two. Using Equation 3.8, and setting r and s both equal to 2, we get:

$$\binom{2+2}{2} = \frac{(2+2)!}{2!2!} = \frac{4 \cdot 3 \cdot 2 \cdot 1}{2 \cdot 1 \cdot 2 \cdot 1} = \frac{24}{4} = 6 \tag{3.9}$$

Similarly, through counting, we can see that a simple 2x3 network should have 3 paths. Setting r equal to 1, and s equal to 2, Equation 3.8 yields:

$$\binom{1+2}{2} = \frac{(1+2)!}{2!1!} = \frac{3!}{2!} = 3 \tag{3.10}$$

Now that we've established the number of paths between a source node and the node under the link, we need to determine the number of paths from the node on the other side of the link to the destination node. With Equation 3.8, we find that the number of paths between the other end of the link, (p, q+1), to the node we are polling, (m,n) is given by:

$$\binom{(m-p)+(n-(q+1))}{m-p} = \frac{(m+n-p-q-1)!}{(n-q-1)!(m-p)!} \tag{3.11}$$

Multiplying Equation 3.7 and Equation 3.11 together, we get the total number of paths between the network management tool and the polled router that cross that link:

$$\binom{p+q}{p}\binom{m+n-p-q-1}{m-p} \tag{3.12}$$

This, divided by the total number of paths between the NMT and the polled host will give us the probability that a path crosses the link $(p,q) \rightarrow (p,q+1)$:

$$\frac{\binom{p+q}{p}\binom{m+n-p-q-1}{m-p}}{\binom{m+n}{m}} \tag{3.13}$$

Now, we can sum the bandwidth used on this link in polling all the mobile hosts. Assume that we have a (h+1)x(k+1) network, with (h,k) being the top right mobile host, and (0,0) being the bottom left mobile host. We know that a packet will always take the shortest path between two hosts, so we can neglect mobile hosts that are closer to the NMS. Hence, the expected number of network management responses over the link above (p,q) in one polling cycle, with V denoting that it is a vertical link, is:

$$\rho^{V}_{(p,q)} = \sum_{n=(q+1)}^{k} \sum_{m=p}^{h} \frac{\binom{p+q}{p}\binom{m+n-p-q-1}{m-p}}{\binom{m+n}{m}} \tag{3.14}$$

The expected high fault detection network management traffic from SNMP responses is:

$$\text{High Priority Fault Detection Traffic}^{V}_{(p,q)} = \left(8\frac{\text{bits}}{\text{byte}} \cdot \rho^{V}_{(p,q)} \cdot \frac{LR_{hpf}}{PI_{hpf}}\right) \text{bps} \tag{3.15}$$

Similarly, the expected traffic generated on any particular link for the topology change detections. Topology change polling must occur every 60 seconds (PI_{tm}), and can be represented by:

$$\text{Topology Change Detection Ttraffic}^{V}_{(p,q)} = = \left(8\frac{\text{bits}}{\text{byte}} \cdot \rho^{V}_{(p,q)} \cdot \frac{LR_{tm}}{PI_{tm}}\right)\text{bps} \tag{3.16}$$

The low priority fault detection must occur every 300 seconds (PI_{lpf}):

$$\text{Low Priority Fault Detection Traffic}^{V}_{(p,q)} = \left(8\frac{\text{bits}}{\text{byte}} \cdot \rho^{V}_{(p,q)} \cdot \frac{LR_{lpf}}{PI_{lpf}}\right)\text{bps} \tag{3.17}$$

Finally, performance management polls must occur every 300 seconds (PI_{pm}):

$$\text{Performance Management Traffic}^{V}_{(p,q)} = \left(8\frac{\text{bits}}{\text{byte}} \cdot \rho^{V}_{(p,q)} \cdot \frac{LR_{pm}}{PI_{pm}}\right)\text{bps} \tag{3.18}$$

Summing these together, we derive the total network management traffic generated by SNMP responses over vertical links:

$$\text{Net Mgt. SNMP Response Traffic}^{V}_{(p,q)} = \left(8\frac{\text{bits}}{\text{byte}} \cdot \rho^{V}_{(p,q)} \cdot BW^{R}_{SNMP}\right)\text{bps} \tag{3.19}$$

Where BW^{R}_{SNMP}, the expected bandwidth per second of the SNMP responses, is defined as:

$$BW^{R}_{SNMP} = \left(8\frac{\text{bits}}{\text{byte}} \cdot \left(\frac{LR_{hpf}}{PI_{hpf}} + \frac{LR_{tm}}{PI_{tm}} + \frac{LR_{lpf}}{PI_{lpf}} + \frac{LR_{pm}}{PI_{pm}}\right)\right)\text{bps} \tag{3.20}$$

Equation 3.19 can be used to deduce the bandwidth over each link *above* the point (i,j), but does not tell us what the bandwidth on the horizontal links are. For horizontal links, the expected number of responses travelling over the link to the right of (i,j) in one polling cycle is:

$$\rho^{H}_{(p,q)} = \sum_{n=(q+1)}^{k} \sum_{m=p}^{h} \frac{\binom{p+q}{p}\binom{m+n-p-q-1}{m-p-1}}{\binom{m+n}{m}} \tag{3.21}$$

The total network management traffic generated by SNMP responses over any given horizontal link to the right of (p,q) is:

$$\text{Net Mgt. SNMP Response Traffic}^{H}_{(p,q)} = (\rho^{H}_{(p,q)} \cdot BW^{R}_{SNMP})\text{bps} \tag{3.22}$$

For a $\sqrt{N} \times \sqrt{N}$ uniform distribution network, $\rho^{V}_{(p,q)}$ and $\rho^{H}_{(p,q)}$ are:

$$\rho^{V}_{(p,q)} = \sum_{n=(q+1)}^{\sqrt{N}-1} \sum_{m=p}^{\sqrt{N}-1} \frac{\binom{p+q}{p}\binom{m+n-p-q-1}{m-p}}{\binom{m+n}{m}} \tag{3.23}$$

$$\rho^{H}_{(p,q)} = \sum_{n=(q+1)}^{\sqrt{N}-1} \sum_{m=p}^{\sqrt{N}-1} \frac{\binom{p+q}{p}\binom{m+n-p-q-1}{m-p-1}}{\binom{m+n}{m}} \tag{3.24}$$

Network management data gathering traffic is centered around (0,0), the mobile host that the NMT is connected to. As an example, for a moderate size 400 node mobile network, the network management bandwidth from each of the two links extending from (0,0) is the maximum of this network. The number of responses that must pass over the two links in one polling cycle is:

$$\rho^{V}_{(0,0)} = \sum_{n=(q+1)}^{\sqrt{400}-1} \sum_{m=p}^{\sqrt{400}-1} \frac{\binom{p+q}{p}\binom{m+n-p-q-1}{m-p}}{\binom{m+n}{m}} = 199.5 \tag{3.25}$$

This number agrees with intuition - we know that for responses to return to (0,0) from the other 399 mobile hosts, half must travel over the link about (0,0), and the other half must travel over the link to the right of (0,0).

In standard SNMP polling, with the values we have attributed to the polling intervals and length of responses:

$$BW^{R}_{SNMP} = 8\frac{bits}{byte} \cdot 8.98\frac{bytes}{second} = 71.9 \text{ bps} \tag{3.26}$$

The total network management SNMP response traffic for the 400 node uniform mobile network over the link above (0,0) is:

$$\text{Net. Mgt. SNMP Response Traffic}^{V}_{(0,0)} = 199.5 \cdot 71.9 = 14339.2\text{bps} \tag{3.27}$$

$$= 14.3\text{kbps}$$

Based on the criteria that network management traffic should compose less than 5% of a network links' overall traffic, and knowing that on the mobile host with the most network management traffic (0,0), each link has network management traffic of 17.9kbps. This implies that each of our network links must have a link rate of 286.8 kbps in each direction, or a total of at least 573.6 bps. This requirement is above the bandwidth provided by BBN's wireless networks.

3.4.2 An elongated network distribution

The second topology is an elongated distribution from one edge to another. A $\frac{\sqrt{N}}{\alpha} \times \alpha\sqrt{N}$ networking topology has the same number of mobile hosts (N), but the diagonal length of the network is longer (Figure 3.3). In other words, the maximum number of hops

that can be taken to get from one corner of the network assuming the shortest path is taken is higher.

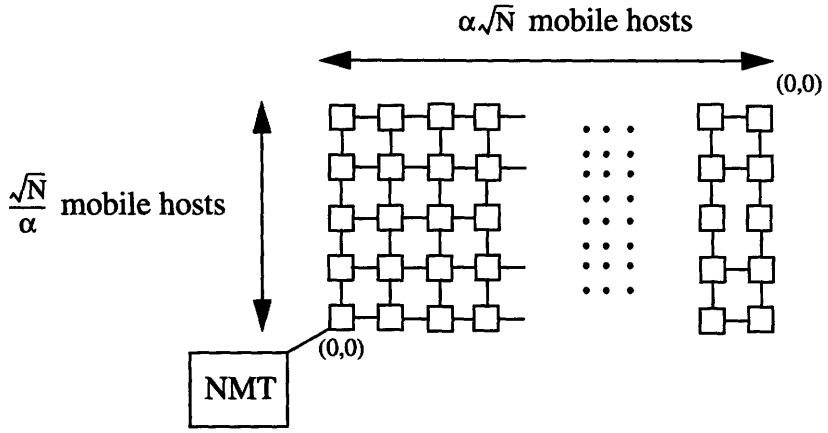

Figure 3.3: An elongated N mobile host distribution

By substituting the following for $\rho^{V}_{(p,q)}$ and $\rho^{H}_{(p,q)}$ in equations Equation 3.19 and Equation 3.22, we obtain equations for network management traffic for any link on a network with a $\frac{\sqrt{N}}{\alpha} \times \alpha\sqrt{N}$ distribution.

$$\rho^{V}_{(p,q)} = \sum_{m=p}^{\alpha\sqrt{N}-1} \sum_{n=q+1}^{\frac{\sqrt{N}}{\alpha}-1} \frac{\binom{p+q}{p}\binom{m+n-p-q-1}{m-p}}{\binom{m+n}{m}} \tag{3.28}$$

$$\rho^{H}_{(p,q)} = \sum_{m=p+1}^{\alpha\sqrt{N}-1} \sum_{n=q}^{\frac{\sqrt{N}}{\alpha}-1} \frac{\binom{p+q}{p}\binom{m+n-p-q-1}{m-p-1}}{\binom{m+n}{m}} \tag{3.29}$$

The maximum network management traffic will flow through the mobile host that the network management station is connected to. Once again, as an example, we consider a moderate sized 400 node mobile network. Using Equation 3.19 and Equation 3.22 with Equation 3.28 and Equation 3.29, we find that the expected number of polls or responses that will traverse the links connected to the mobile host that the NMS is connected to, with α set to 4 (i.e. a 5x80 network):

$$\rho^{V}_{(0,0)} = \sum_{m=0}^{\alpha\sqrt{400}-1} \sum_{n=1}^{\frac{\sqrt{400}}{\alpha}-1} \frac{\binom{p+q}{p}\binom{m+n-p-q-1}{m-p}}{\binom{m+n}{m}} = 36.07 \tag{3.30}$$

$$\rho^{H}_{(0,0)} = \sum_{m=1}^{\alpha\sqrt{N}-1} \sum_{n=0}^{\frac{\sqrt{N}}{\alpha}-1} \frac{\binom{p+q}{p}\binom{m+n-p-q-1}{m-p-1}}{\binom{m+n}{m}} = 362.93 \tag{3.31}$$

As a check, we see that the sum of the expected number of polls and requests that go through the link above (0,0) and the link to the right of (0,0) is 399.

We also see that it is expected that more network management traffic will flow over the horizontal link adjacent to (0,0). Using that as a threshold, we find that the total traffic floating over that link is expected to be:

$$\text{Net. Mgt. SNMP Response Traffic}^{V}_{(p,q)} = 362.93 \cdot 71.9\text{bps} = 26085.8 \text{ bps} \tag{3.32}$$

$$= 26.1 \text{ kbps}$$

To contain network management traffic to 5% of total bandwidth of this link, every this link needs to allow at least 521.7 kbps in each direction.

3.5 General conclusions

For any given network distribution, the bandwidth used by network management traffic increases linearly with the number of mobile hosts in the network. The amount of bandwidth needed per link increases linearly as a function of number of mobile hosts also.

Quantitatively, the minimum amount of network management traffic from SNMP responses is:

$$\text{Net Mgt. SNMP Response Traffic} = \left(\frac{\text{N-1}}{\text{NMS}_{\text{links}}} \cdot \text{BW}^{R}_{\text{SNMP}}\right)\text{bps} \tag{3.33}$$

With four links from each mobile host, and the NMS on a corner, at least half of the polls and responses passing over the link with the maximum network management traffic, so $NMS_{links}=2$. In mobile wireless networks with the NMS in the center of the network instead of the corner can have $NMS_{links}=4$, and one of the edge of the network (but not a corner) can have $NMS_{links}=3$.

The maximum number of polls that have to pass over a link is N-1 (for a completely elongated 1xN network). The network management SNMP response traffic in that case is:

$$\text{Net Mgt. SNMP Response Traffic} = ((N-1)\cdot BW_{SNMP}^{R})\text{bps} \tag{3.34}$$

Chapter 4

Alternative network management data gathering solutions

4.1 Introduction

In this chapter we first discuss bandwidth usage of standard SNMP polling over BBN's mobile wireless network. We then propose three alternative strategies to standard SNMP polling - adaptive SNMP, proxy server SNMP, and a hybrid SNMP/OSPF network data gathering strategy - and analyze the bandwidth used by each.

4.2 Standard SNMP polling

As described in Chapter 1, standard SNMP relies on polls and responses for obtaining information from the network. The traffic generated by standard SNMP polling has been described in Chapter 3, and is summarized in Table 4.1.

Poll type	# of polls per MH	PI per poll (sec.)	LP per poll (bytes)	LR per poll (bytes)	Total LP per MH	Total LR per MH
hpf	1	30	73	73	73	73
lpf	4	300	73	73	292	292
tm	4	60	73	77	292	308
pm	10	1800	73	80	730	800

Table 4.1: Standard SNMP polling traffic table

As shown in Chapter 3, Equation 4.1 describes the traffic flow over the link with the maximum network management traffic:

$$\text{Net Mgt. SNMP Response Traffic}_{max} = (\rho_{max} \cdot BW^{R}_{SNMP})\text{bps} \quad (4.1)$$

Where:

$$\rho_{max} = max(\rho^{V}_{(0,0)}, \rho^{H}_{(0,0)}) \text{ and } BW^{R}_{SNMP} = 8\frac{\text{bits}}{\text{byte}} \cdot \left(\frac{LR_{hpf}}{PI_{hpf}} + \frac{LR_{tm}}{PI_{tm}} + \frac{LR_{lpf}}{PI_{lpf}} + \frac{LR_{pm}}{PI_{pm}}\right) = 71.9 \text{ bps}$$

The value of ρ_{max} can range from $\frac{N-1}{NMS_{links}}$ to N-1, depending on the number of links extending from the mobile host that the NMS is connected to (Equation 4.2).

$$\frac{N-1}{NMS_{links}} < \rho_{max} < N-1 \quad (4.2)$$

As mentioned in the conclusion of Chapter 3, for the purpose of our analysis, we will focus solely on $\rho=\rho_{max}=N$, the worse case scenario. Hence:

$$\text{Net Mgt. SNMP Response Traffic}_{max} = 71.9\text{bps} \cdot (N-1) \quad (4.3)$$

4.3 Adaptive SNMP polling rate

In the previous chapter we discussed the possibility that network topology may be changing more frequently than the up/down status of a mobile host. This implies that the lower bound on the interval of time between SNMP polls may be dictated more by how quickly the network is changing rather than how often a mobile host fails. In real world wireless networks there may be some fraction of the mobile hosts that is currently mobile, while the remainder are stationary.

Adaptive SNMP polling hopes to exploit the fact that a subset of mobile hosts are immobile and do not need to be polled for topology changes as often as the subset that is mobile. This algorithm assumes that if a mobile host is immobile for a predefined period of time, there is a high likelihood that it will remain immobile. By polling the stationary

hosts for topology changes with a longer polling interval, we can lower network management traffic generated for topology detection.

4.3.1 An algorithm for detecting no changes

The algorithm below detects that a host has been immobile for an extended period of time, and lengthens the period of time between SNMP polls.

```
#define NUMBER_OF_MOBILE_HOSTS 400
#define MAXIMUM_POLLING_INTERVAL 300

/* poll_interval is an array with the index representing the router
    index's current polling interval */

double poll_interval[NUMBER_OF_MOBILE_HOSTS];
int i;

/* Initially the polling interval for each mobile host is 60 sec-
    onds */

for (i=0; i++; i<NUMBER_OF_MOBILE_HOSTS)
    poll_interval[i] = 60;

while 1{
    for (i=0; i++; i<NUMBER_OF_MOBILE_HOSTS){
        if (mobile_host_moved(i) == 0)
            if (poll_interval[i] < MAXIMUM_POLLING_INTERVAL)
                poll_interval[i] = poll_interval[i]*1.10;
        if (mobile_host_moved(i) == 1)
            poll_interval[i] = 60;
    }
    sleep 60;}
```

The variable, poll_interval, is shared between this thread and another thread which is responsible for invoking the polling client. Hence, with this algorithm, after a poll in which the mobile host has not moved since the last poll, the time interval till the next poll will increase by 10%, up to 300 seconds. If the mobile host has moved since the last poll, the poller assumes that the router may continue to move, and resets the polling interval at 60 seconds.

4.3.2 Bandwidth usage

The bandwidth used by this method is difficult to determine because the amount of polling traffic generated is dependent on mobility of the network. When the algorithm first starts off, bandwidth usage is the same as in the standard SNMP polling. With the algorithm described in Section 4.3.1, the network management data gathering tool only lowers the interval at which it's polling if a mobile host does not move in 60 seconds[1]. If all the nodes in the network are always moving every 60 seconds, then the polling interval will never change, and bandwidth usage will remain the same as the standard SNMP polling.

In this analysis, we will use β to represent the fraction of mobile hosts that are currently moving or have moved around in the last 17 minutes, and 1-β equals the fraction of mobile hosts that have been immobile for 17 minutes (i.e. mobile hosts whose polling interval is MAXIMUM_POLLING_INTERVAL seconds). We will use PImax-tm to represent the new maximum topology management polling interval for stationary polling mobile hosts.

For every 60 seconds that no mobile hosts are moving, the polling interval is increased by 10% until it reaches the maximum value set in the algorithm. To reach the maximum of 300 second polling interval used in the adaptive SNMP polling algorithm, a mobile host in the network must remain immobile for at least 17 minutes. Assuming this maximum polling interval is reached, the network management traffic will consist of low priority fault detection every 5 minutes, high priority fault detection every 30 seconds, and topology detection every 300 seconds (the standard SNMP polling rate for topology detection is 60 seconds). The network management traffic generated by the responses to SNMP polls becomes:

1. This 60 second interval is configurable as seen fit by the network manager.

$$\text{A-SNMP Response Traffic}_{max} = \rho_{max} \cdot BW_{A\text{-}SNMP}^{max} \tag{4.4}$$

$$BW_{A\text{-}SNMP}^{max} = 8\frac{bits}{byte} \cdot \left(\frac{LR_{hpf}}{PI_{hpf}} + \frac{LR_{lpf}}{PI_{lpf}} + \frac{LR_{pm}}{PI_{pm}} + \beta\left(\frac{LR_{tm}}{PI_{tm}}\right) + (1-\beta)\left(\frac{LR_{tm}}{PI_{max\text{-}tm}}\right)\right) bps \tag{4.5}$$

In the best case of all the hosts being immobile, with β=0, SNMP response traffic becomes:

$$\text{A-SNMP Response Traffic}_{max} = (N-1) \cdot 8 \cdot \left(\frac{LR_{hpf}}{PI_{hpf}} + \frac{LR_{lpf}}{PI_{lpf}} + \frac{LR_{pm}}{PI_{pm}} + \frac{LR_{tm}}{PI_{max\text{-}tm}}\right) = 39 \cdot (N-1) \tag{4.6}$$

In the worse case of all the hosts frequently moving, with β=1, SNMP response traffic becomes the same as standard SNMP polling:

$$\text{A-SNMP Response Traffic}_{max} = (N-1) \cdot BW_{SNMP}^{max} = 71.9 \cdot (N-1) \tag{4.7}$$

Adaptive SNMP produces at best 46% less network management response traffic than standard SNMP polling.

The general equation for the maximum network management traffic used by responses in adaptive SNMP polling, as a function of β is:

$$(\text{A-SNMP Response Traffic}_{max} = (N-1) \cdot (39 + \beta(32.9)) \text{ bps}) \tag{4.8}$$

A summary of the number of polls, polling intervals, size of polls, and size of packets

Poll type	# of polls per MH	PI per poll (sec.)	LP per poll (bytes)	LR per poll (bytes)	Total LP per MH (bytes)	Total LR per MH (bytes)
hpf	1	30	73	73	73	73
lpf	4	300	73	73	292	292
tm	4	$60\beta+300(1-\beta)$	73	77	292	308
pm	10	1800	73	80	730	800

Table 4.2: Traffic generated with Adaptive SNMP polling

for the different poll types is provided in Table 4.2.

4.3.3 Future considerations

It is possible that we can develop a deterministic pattern involving when (specific times of the day, specific days of the week, etc.) topology changes are more frequent. With that further information embedded within the network poller, we can anticipate when we will have to poll less frequently, hence lowering overall polls on the network. Also, if we know when the network mobility increases again, we can allow the maximum poll interval to decrease, and then have it automatically lowered *before* the mobile hosts become mobile again.

4.4 Network management proxying

SNMP's polling intensive nature requires that its use be efficiently managed over wireless links [7]. In networks that are a hybrid of low speed wireless and high speed wireline links, one common strategy for lowering the number of polls over wireless links is to

going onto the wireless links when possible. A proxy agent responds to SNMP requests for static information about the mobile host, and passes to the mobile hosts the SNMP requests that are related to the dynamic mobile host information [7]. With this setup, polling over bandlimited wireless links only occurs when the information is not available on the wireline connected proxy server. The proxy server's role is similar to that of a cache, in that it provides quicker more responsive, albeit sometimes staler, data without adding load to the wireless network. We can use a slight variation of the proxy server idea to lower network management traffic over mobile wireless mobile networks.

Instead of having one proxy server on a wireline network responsible for a group of wireless mobile hosts, we can have one of the mobile hosts acting as a proxy server for a group of mobile hosts. When the network management tool wants information about the mobile hosts the proxy server mobile host is responsible for, it polls each proxy server mobile hosts and requests information about the mobile hosts in it's group. Hence, only one poll is needed to ascertain the status of a group mobile hosts.

4.4.1 Proxy server mechanism

For proxy serving to occur, the mobile hosts first need to be divided into groups within which one mobile host acts as a proxy server and responds to the network management station's SNMP queries to the other mobile hosts in the group. The process of establishing these groups and choosing a mobile host as the proxy server for the group is complex. For the purposes of this thesis, we will assume that an algorithm exists to do optimally do this.

The network management tool must be aware of which mobile hosts are acting as proxy servers, and which mobile hosts are in each group associated with the proxy server.

One possible way to do this is to have the proxy server send a short message to the NMS establishing itself as a proxy server that needs to be polled.

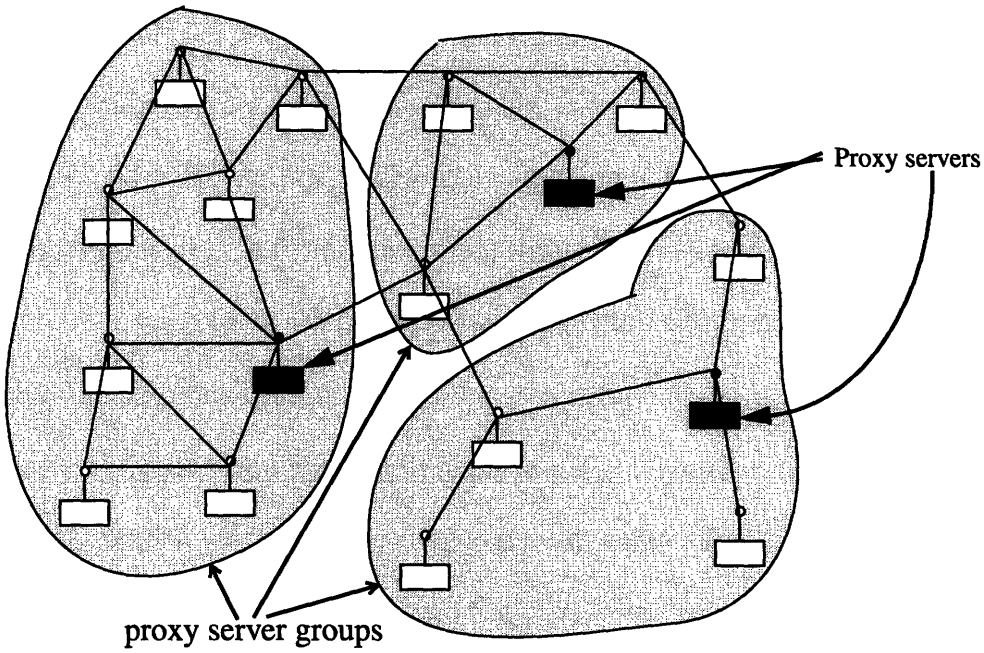

Figure 4.1: Example SNMP proxy serving network without clustering

Each proxy server has the responsibility of keeping a record of the state of each of the mobile host within it's cluster. They must each:

1. Use SNMP to:

    a. Retrieve and store information regarding which mobile hosts in its cluster are currently up (high priority faults).

    b. Gather information about low priority faults from cluster members.

    c. Gather topology information from cluster members.

2. Respond to SNMP queries from network management station concerning any of the routers it is responsible for.

4.4.2 Bandwidth usage

For the purposes of this analysis, we will assume that the grouping algorithm assigns M mobile hosts to each of G groups, with one mobile host in each group acting as the proxy server. So, $N = G \cdot M$.

The NMS must poll G proxy servers, and each proxy server must poll M-1 other members of its group. To ease analysis, we will assume that each proxy server is on the lower left of the group. For example, in a 6x6 network, the proxy servers would be as shown in Figure 4.2. For this example, N=36, G=4, and M=9.

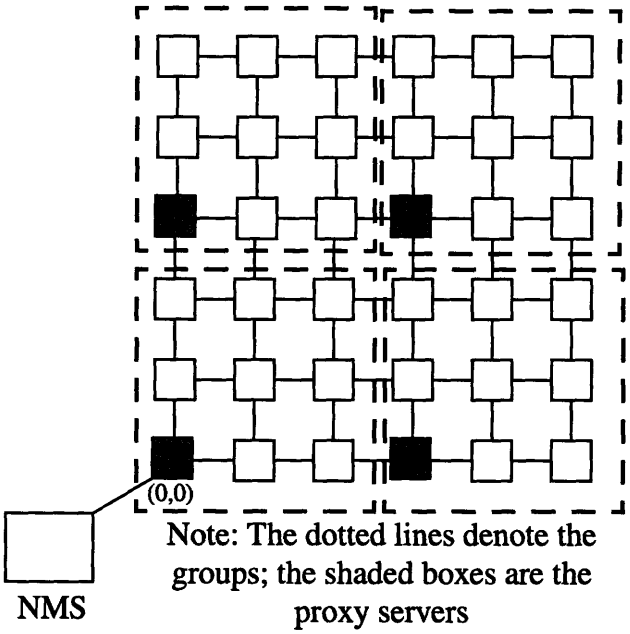

Figure 4.2: A 6x6 proxy server network

Each proxy server must gather data from it's cluster members just as an NMS would gather data from a M mobile host network, and the size of the SNMP packets as well as the polling intervals or the two are identical (Table 4.3).

Poll type	# of polls per MH	PI per poll (sec.)	LP per poll (bytes)	LR per poll (bytes)	Total LP per MH	Total LR per MH
hpf	1	30	73	73	73	73
lpf	4	300	73	73	292	292
tm	4	60	73	77	292	308
pm	10	1800	73	80	730	800

Table 4.3: Polls from proxy server to cluster members

The NMS uses SNMP to poll each of the G proxy servers every PI_{hpf} seconds to obtain high priority fault information for it and its group members. Each proxy server returns an SNMP response with information indicating which mobile hosts in its group are up, and which mobile hosts in its group are down. The polls do not need to contain much information, so each of them is approximately 73 bytes (LP_{hpf}). In the response, the proxy server should package the information about the high priority faults of the group members into a single SNMP response packet. Hence, each response is approximately the size of a generic SNMP response (73 bytes) plus data needed to include the up/down status of each of the group members. The proxy server needs to return the IP address and up/down status of each of the M group members. Each group member entry in the SNMP response packet is approximately 5 bytes (IP address plus up/down status), so the total size of the response packet is approximately $73 \text{ bytes} + (5 \text{ bytes} \cdot \text{M group members})$ bytes (LR_{hpf}^{proxy}).

The NMS also uses SNMP to poll the proxy servers for information about low priority faults in the cluster every PI_{lpf} seconds. Once again, the SNMP polls do not need to con-

tain a lot of information, and are approximately 73 bytes (LP_{lpf}) in length. As previously stated, we are assuming that the NMS needs to monitor the up/down status of 4 local interfaces on each mobile host. Each interface's entry in the SNMP response packet is 5 bytes. Therefore, the total size of the response packet is approximately $73\text{bytes}+(5\text{bytes} \cdot 4\text{interfaces} \cdot M)$ bytes (LR_{lpf}^{proxy}).

To monitor topology the NMS must monitor each proxy server every PI_{tm} seconds. The SNMP poll to the proxy server is approximately 73 bytes (LP_{tm}). The proxy server constructs and returns one SNMP response packet with all the topology information for its group. The response contains M entries (one for each member of the group), and assuming a mobile host has an average of four connections, the size of each entry is 20 bytes (4 bytes for the IP address of the mobile host, and 4 sets of 5 bytes each for each of the mobile hosts it is connected to). The total number of bytes that need to be returned in one SNMP poll response is $73\text{bytes}+(20\text{bytes} \cdot (\text{M mobile hosts}))$ bytes (LR_{tm}).

Performance management variables must be obtained every PI_{pm} seconds. We previously stated that each mobile host has 10 such variables that need to be monitored. Each of the values for these variables is on the average 4 bytes. So, for each group member, we need to return 40 bytes of data. The total size of the SNMP response from the proxy server to the NMS is $73 \text{ bytes}+\left(4\frac{\text{bytes}}{\text{variable}}\right)\cdot(10 \text{ variables}) \cdot (\text{M cluster members})$ bytes (LR_{pm}^{proxy}).

A summary of these defined variables for the different polling types in wireless mobile networks is provided in Table 4.4.

Poll type	# of polls per proxy server	PI (sec)	Total LP^{proxy} (bytes)	Total LR^{proxy} (bytes)
hpf	1	30	73	73+(5)(M)
lpf	1	300	73	73+(5)(M)
tm	1	60	73	73+(20)(M)
pm	1	1800	73	73+(40)(M)

Table 4.4: Traffic from SNMP proxy serving

As seen in Figure 4.2, the mobile host that the NMS is connected to (0,0) not only sends the NMS's queries to the proxy servers, but because it is also acting as a proxy server, it must poll all its group members. Hence, its links have the most network management traffic flow in responses (the sum of the proxy server polls and the group member polls). In the case of the proxy server network management strategy:

$$BW^{max}_{proxy\text{-}total} = BW^{R}_{SNMP} + 8\frac{bits}{byte}\left(\frac{LR^{proxy}_{hpf}}{PI_{hpf}} + \frac{LR^{proxy}_{lpf}}{PI_{lpf}} + \frac{LR^{proxy}_{pm}}{PI_{pm}} + \frac{LR^{proxy}_{tm}}{PI_{tm}}\right) \tag{4.9}$$

To determine the optimal number of groups, we need to minimize the traffic flowing over the links on the mobile host that the NMS is connected to. That is, we need to find the minimum of:

$$(M-1)\cdot BW^{R}_{SNMP} + (G-1)\cdot 8\frac{bits}{byte}\left(\frac{LR^{proxy}_{hpf}}{PI_{hpf}} + \frac{LR^{proxy}_{lpf}}{PI_{lpf}} + \frac{LR^{proxy}_{pm}}{PI_{pm}} + \frac{LR^{proxy}_{tm}}{PI_{tm}}\right) \tag{4.10}$$

Substituting for the polling intervals and lengths of the responses, and setting the first derivative with respect to M equal to 0, we find that the optimal M is:

$$M = 0.488 \cdot \sqrt{N} \tag{4.11}$$

and G becomes:

$$G = 2.05 \cdot \sqrt{N} \tag{4.12}$$

Both G and M need to be chosen as integers that best fit Equation 4.11 and Equation 4.12.

The total SNMP traffic from responses to SNMP queries becomes:

$$\text{SNMP Response Traffic}_{max} = ((G-1) \cdot BW^{R}_{proxy}) + ((M-1) \cdot BW^{R}_{SNMP}) \tag{4.13}$$

$$BW^{R}_{proxy} = 8 \cdot \left(\frac{LR^{proxy}_{hpf}}{PI_{hpf}} + \frac{LR^{proxy}_{lpf}}{PI_{lpf}} + \frac{LR^{proxy}_{tm}}{PI_{tm}} + \frac{LR^{proxy}_{pm}}{PI_{pm}} \right) = (31.47 + (4.31 \cdot M)) \text{ bps} \tag{4.14}$$

Substituting for G, M, and BW_{SNMP} in Equation 4.13:

$$\text{SNMP Res. Traf.}_{max} = ((2.05 \cdot \sqrt{N}) - 1) \cdot (31.5 + (4.31 \cdot 0.49 \cdot \sqrt{N})) + ((0.49 \cdot \sqrt{N}) - 1) \cdot 71.9 \tag{4.15}$$

$$= (((97.5 \cdot \sqrt{N}) + 4.3 \cdot N) - 103.4) \text{ bps}$$

4.4.3 Other considerations

The optimal grouping sizes derived in the previous section are assuming the worse case completely elongated network distribution. This optimal value changes if the number of links extending from the NMS's mobile host is not equal to the number of links extending from each proxy server's mobile host. A consideration for future work is a dynamic grouping algorithm that executes an optimal grouping strategy based on the current network topology.

4.5 Using OSPF routing updates to do network management

The Open Shortest Path First (OSPF) protocol is an interior gateway protocol (IGP) based on the link state or shortest path first (SPF) algorithm. It was developed in response to a need in the Internet community to introduce a high functionality non-proprietary IGP for the TCP/IP protocol family. It was introduced as a replacement for the Bellman-Ford algorithm used in traditional TCP/IP routing protocols (i.e. RIP). Some of its advantages include a quick convergence after changes in network topology (routing changes are propagated instantaneously, not periodically), and it's scalability (unlike RIP, there is no limitation on number of hops beyond which a node is considered unreachable). In wireless networks with mobile hosts that are constantly in transit the rapid convergence becomes a necessity, hence OSPF is a likely candidate for wireless networks.

OSPF's distributed link state advertisement mechanism makes some of its functionality an ideal replacement for some network management responsibilities. A topology map can be constructed by having the network management station listen to link state updates.

4.5.1 OSPF overview

Link state protocol. OSPF is a link state protocol. A link in a wireless network is a wireless virtual connection between two mobile hosts. The state of the link include the IP addresses of the two endpoints of the connection, the subnet mask, the network it is connected to, and various other tidbits. The collection of all the links in an autonomous system (AS)[1] forms the link state database.

OSPF uses a link state shortest path first algorithm to calculate the shortest path between any source and destination. From a high level view, this algorithm functions as follows:

1. *Autonomous system* - A group of routers or mobile hosts exchanging routing information via a common routing protocol. In our discussion, we consider the entire network to be one AS.

1. Upon initialization, each mobile host generates a link state advertisement that represents all the link states on that mobile host.

2. All mobile hosts exchange link states by means of flooding. Every mobile host that receives a copy of a link state update checks to see if it is a duplicate (thus eliminating loops), stores it, and forwards it on to its neighbors.

3. Each mobile host uses Dijkstra's algorithm to calculate a shortest path tree to all destinations, and uses that to form its routing table.

4. When there is a change in a mobile host's link state, it sends a link state update to all its neighbors, and Dijkstra's algorithm is used to recalculate the shortest paths.

Areas. To prevent the flooding of link state updates throughout the whole network, OSPF allows the subdivision of networks into separate autonomous systems called areas. Area border routers (ABR), or routers that are in multiple autonomous systems, are responsible for acting as gateways between for disseminating routing information between areas. The boundaries between autonomous systems are statically assigned before network deployment. The mobility of wireless networks makes it unviable to partition wireless networks into autonomous systems, so for this strategy we are assuming that we are dealing with one AS.

Link state advertisement packets. There are four different types of link state advertisement packets - router link advertisements, summary link advertisements, network link advertisements, and external link advertisements. We are only focusing on the router links, which, as described before, are generated by the mobile hosts. The summary links are only advertised by ABRs (are only required if there are multiple autonomous systems), and network links are only necessary for multi-access segments with more than one router. External links are advertised if a wireless network has routes to outside external networks. For the purposes of network management of wireless networks, we are assuming that the network management station is only monitoring mobile hosts within the wireless network.

Neighbors. To establish what links a mobile host has up and down, each mobile host exchange Hello messages with its neighbors at periodic intervals. When a mobile host has not received a Hello message within a prescribed time interval, it generates a link state advertisement that propagates throughout the network. The period of time between transmission of Hello messages is configurable, and is generally set at to be less than 15 seconds in networks that are constantly changing.

4.5.2 Using OSPF udates for network management

Each mobile host maintains a constant topology map of the entire network by listening to OSPF link state updates. Routing tables in networks running OSPF converge very quickly - usually within seconds of mobile host determining that one of its neighbors is no longer connected to it. With a Hello message being sent every 15 seconds, the entire network is aware of any changes in topology within a few seconds after that through flooding.

The OSPF network managment strategy is to have the network management data collection unit listen to the OSPF link state advertisements, and filter back network management information to the station. If a mobile host experiences a high priority fault (it loses power, is completely incapacitated, etc.), its neighbors will detect this after not receiving a Hello message in the prescribed 15 second period and will flood the network with a link state advertisement. In the OSPF network management strategy, the network management data collection unit listens to this advertisement, and discerns that the mobile host is down. The NMS receives this information within the information model requirement of 30 seconds for high priority network faults.

Similiarly, if there is a change in topology, the NMS will be aware of this within 30 seconds of the change by listening to OSPF routing updates. To OSPF, a change in topology generates two link state advertisements. In Figure 4.3, when MH5 moves and loses

connectivity to MH3, MH3 generates a link state advertisement indicating that it no longer has a connection to MH5, and floods the network with the update. All the other mobile

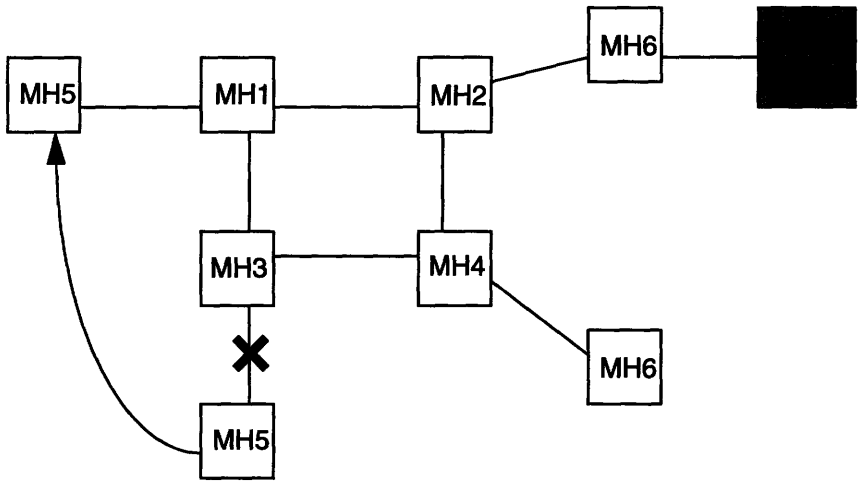

Figure 4.3: Change in network topology. MH5 moves, loses connectivity to MH3, and initiates connection with MH1

hosts in the network and the NMS update their topology databases to reflect this change. Next, when MH5 initiates a connection with MH1, and begins transmitting Hello packets to it, MH1 generates a link state advertisement describing this new link, and floods the network with it. The NMS receives this and updates its topology database to reflect the new connection. The link state advertisements reflected these changes will be flooded throughout the network within 30 seconds, putting topology change detection with the OSPF strategy well within the 60 second requirement for detecting network topology changes.

4.5.3 Bandwidth usage

As shown in Section 4.5.2, high priority network faults and changes in topology can be detected within the time periods required by the information model. Standard SNMP tools must be used to detect low priority faults and to do performance management (Table 4.5).

Poll type	# of polls per MH	PI per poll (sec.)	Total LP per poll (bytes)	Total LR per poll (bytes)	Total LP (bytes)	Total LR (bytes)
hpf	0	-	0	0	0	0
lpf	4	300	73	73	292	292
tm	0	-	0	0	0	0
pm	10	1800	73	80	730	800

Table 4.5: Traffic from using OSPF updates for network management

There is no new network management traffic introduced when we listen to the OSPF routing updates. The worse case total bandwidth consumed by SNMP responses becomes:

$$\text{OSPF SNMP Response Traffic}_{max} = \rho_{max} \cdot BW_{OSPF\text{-}SNMP} \tag{4.16}$$

$$BW_{OSPF\text{-}SNMP} = 8\frac{bits}{byte} \cdot \left(\frac{LR_{lpf}}{PI_{lpf}} + \frac{LR_{pm}}{PI_{pm}}\right) = 11.34 \text{ bps} \tag{4.17}$$

In the worse case, the bandwidth consume by OSPF becomes:

$$\text{OSPF SNMP Response Traffic}_{max} = (N-1) \cdot 11.34 \text{ bps} \tag{4.18}$$

4.6 Summary

The following table is a summary of the maximum bandwidth consumed with ρ_{max}=N, the

worse case network scenario.

Net. Mgt. Strategy	Max. bandwidth consumed (bps)
Standard SNMP polling	$71.9 \cdot (N-1)$
Adaptive SNMP polling	$(39 + \beta(32.9)) \cdot (N-1)$
SNMP proxy serving	$(((97.5 \cdot \sqrt{N}) + 4.3(5.2) \cdot N) - 103.4)$ bps
OSPF strategy	$11.34 \cdot (N-1)$

Table 4.6: Summary of traffic usage for different network management strategies

Chapter 5

Guidelines for choosing a network management strategy

5.1 Introduction

Chapter 4 presented three alternate strategies to standard SNMP polling on mobile wireless networks - adaptive SNMP polling, proxy serving SNMP requests, and using OSPF routing updates to do network management. Each of these strategies has its advantages and disadvantates. This chapter will provide a guide for network architects and network management planners in choosing an adequate network management strategy for their wireless networking needs.

5.2 Steps for choosing a network management strategy

As shown in chapters 2, 3, and 4, various parameters effect the bandwidth consumed by network management traffic in mobile wireless network management traffic. These parameters include the polling intervals, length of the polls, number of nodes, topology, link rate, and mobility.

When choosing a network management strategy for a wireless network, the first step is to identify the key network parameters:

1. The link rate of the network needs to be identified. Given that, we can calculate what amount of network management traffic will allow us to remain beneath the 5% network management traffic maximum for mobile wireless networks. In the case of BBN's mobile wireless network, the link rate is 50 kbps.

2. The wireless network manager must then identify a range for the number of mobile hosts in the wireless network.

3. A value for the mobility variable needs to be estimated. The mobility variable is an estimation of the fraction of mobile hosts that are expected to be mobile for more than the maximum polling interval (defined as PImax-tm seconds in Chapter 4).

It is necessary to define values for the information model parameters. Specifically, the network manager needs to set bounds for notifications (by setting the polling interval) of:

1. High priority faults
2. Low priority faults
3. Topology changes
4. Performance management

The lengths of the polls and responses can be modified by adjusting the number of interfaces that need to be monitored for low priority faults on each mobile host, or to add or remove performance variables from the performance management data set.

Using these parameters with the equations derived in Chapters 3 and 4, the maximum bandwidth used by network management traffic over any link can be calculated for each of four strategies (standard SNMP and its alternatives). For a given strategy, if the maximum bandwidth required is 5% or less of the link rate of the network, then that strategy is feasible.

Finally, each feasible strategy needs to be evaluated for other costs and benefits that are not associated with network management traffic bandwidth restrictions. These evaluations are more qualitative than quantitative, and the network manager should use discretion in weighing the costs and benefits for each strategy.

Given the set of parameters for the network structure and characteristics, and information requirements, the following sections show which network management strategies are feasible for which networks. Each strategy is followed by a subsequent discussion of various other costs and benefits associated with it, along with an evaluation with general tips.

5.3 Standard SNMP polling

The maximum network management traffic in standard SNMP polling given the parameter values chosen in Table 4.1 is:

$$\text{Max. network mgt. traffic} = ((N-1) \cdot 71.9) \text{ bps} \tag{5.1}$$

The link rate required to sustain this network management traffic at 5% of the network link's total bandwidth is:

$$\text{Required link rate} = \text{Max. network mgt. traffic} \cdot 20 = (1438 \cdot (N-1)) \text{ bps} \tag{5.2}$$

For BBN's mobile wireless network's 50 kbps duplexed links in each direction, this implies that in the worse case network scenario, we can monitor 35 mobile hosts (Equation 5.3).

$$N = \frac{50000 \text{ bps}}{1438 \text{ bps}} + 1 \approx 35 \text{ mobile hosts} \tag{5.3}$$

5.3.1 Advantages

SNMP is a time tested network management protocol. Years of use have proved it to be reliable, and the problems and deficiencies that haven't been ironed out of it are well known.

There are no added implementation costs. Because the technology is not new, almost all major network devices support it, as well as all popular network management tools.

Its open data structures make it easy to add more network management variables without extensive modification of the software.

5.3.2 Disadvantages

As discussed in Chapter 1, SNMP's polling intensive nature causes it to inefficiently consume large amounts of bandwidth.

5.3.3 Evaluation

If the mobile wireless network has the bandwidth to spare, this is an easy and straightforward strategy. However, if there are plans to increase the network size, thus increasing the number of polls that need to be made to monitor all the mobile hosts, it may be worthwhile to invest it a more scalable strategy.

5.4 Adaptive SNMP polling

Unlike other strategies, adaptive SNMP polling is dependent on the fraction of mobile hosts that have been immobile for the maximum polling interval, $PI_{max\text{-}tm}$. The maximum network traffic using the parameter values given in Table 4.2 is:

$$\text{Max. Net. Mgt. Traffic} = ((N-1)\cdot(39+\beta(32.9))\text{ bps}) \tag{5.4}$$

To maintain the 5% restriction on network management response traffic overhead, we need links rates of:

$$\text{Required link rate} = \text{Max. network mgt. traffic} \cdot 20 \tag{5.5}$$

$$= (N-1)\cdot(39+\beta(32.9))\cdot 20 = (N-1)\cdot(780+\beta(658))\text{ bps} \tag{5.6}$$

If the mobility (β) of the network is completely unpredictable, or there is no upper bound on its value, then this strategy cannot be implemented with a guarantee of containing network management traffic overhead to 5% of overall network traffic. In other words, to maintain the 5% guarantee, we would need to assume that β=1.

Assuming a β=0.5, and duplexed links that support 50 kbps in each direction, we can support 46 mobile hosts using this network management strategy (31% more than standard SNMP polling):

$$N = \frac{50000\text{ bps}}{780+(0.5)(658)} + 1 \approx 46\text{ mobile hosts} \tag{5.7}$$

In the best case of β=0, and duplexed links that support 50 kbps in each direction, we can support 64 mobile hosts with this network management strategy (83% more than standard SNMP polling):

$$N = \frac{50000 \text{ bps}}{780} + 1 = 64 \tag{5.8}$$

In the worse case of β=1, we can support the same number of mobile hosts that the standard SNMP polling algorithm can support (35 mobile hosts).

5.4.1 Advantages

The adaptive SNMP strategy provides all functionality of SNMP. It's simple, we know it works and is reliable, it provides the required information, and it's easily estensible to new networking devices.

Only the software on the network management station needs to be modifed to implement this strategy. The mobile hosts' software does not need to be changed.

Assuming $\beta \neq 1$, this strategy requires less bandwidth than standard SNMP polling.

5.4.2 Disadvantages

When the polling interval reaches a maximum length, there is a delay in detecting a change in network topology. So if a mobile host has been immobile for enough time for $PI_{max\text{-}tm}$ to have been reached, the expected time till detection of a topology change is $\frac{PI_{max\text{-}tm}}{2}$ instead of $\frac{PI_{tm}}{2}$.

The implementation of the adaptive SNMP polling mechanism requires that the data gathering engine of the network management be modified to poll at a varying rate.

5.4.3 Evaluation

The costs associated with the implementation may not be very high. Most network management tools are designed in a modular fashion, so the modification of the network management data collection tool's polling module should be a relatively straightforward task.

The timeliness of the response with this solution is similiar to the timeliness of responses with constant polling. If mobile hosts in a network are moving around, then the polling interval will remain low and changes will be noted. If the mobile hosts are not moving, then the polling interval will be long, and changes will not need to be noted. The problem occurs at the transition periods - when the status of a mobile host's position has been stable for a long enough period of time to reach the maximum polling interval, and then a link is broken or one is added. In this case, it may take 300 seconds for link information to get back to the network management client. Actual observed topology dynamics for a particular wireless network need to be analyzed before deciding what the maximum polling interval should be, and what percentage changes in the polling interval need to occur in each iteration of the polling cycle. If these delays in topology detection are unacceptable, this solution is not acceptable.

Finally, if the mobility of a network cannot be predicted, the upper bound on the amount of network management traffic generated by this strategy is equal to the amount of network management traffic generated by standard SNMP polling. Hence, we must expect that only 35 nodes can be monitored.

5.5 Proxy servers

Assuming optimally chosen group sizes, the maximum bandwidth used by the proxy server network management mechanism is (from Table 4.3 and Table 4.4):

$$\text{Max. Net. Mgrt Traffic}_{\text{proxy server}} = (((97.5 \cdot \sqrt{N}) + 4.3 \cdot N) - 103.4) \tag{5.9}$$

To support this network management mechanism while adhering to the 5% restriction on network management traffic overhead, we must have a link rate of:

$$\text{Link rate} = (((97.5 \cdot \sqrt{N}) + 4.3 \cdot N) - 103.4) \cdot 20 \tag{5.10}$$

Therefore, using optimally chosen group sizes, and a duplexed link rate of 50 kbps in each direction, we find we can support 248 hosts (a gain of 609% over standard SNMP polling):

$$N \approx 248 \text{ mobile hosts} \tag{5.11}$$

5.5.1 Advantages

This strategy lowers the bandwidth consumed by network management traffic significantly more than the other strategies presented in this chapter, and allows more than 6 times as many hosts to be monitored over 50 kbps links.

Additionally, BBN plans to incorporate clustering into their network at a future date, and this SNMP proxy server strategy fits naturally into the architecture of mobile wireless ad hoc networks with clustering. The clusters can play the role of SNMP proxy server groups, and the cluster heads can act as proxy servers.

5.5.2 Disadvantages

Depending on how long it takes to stage the data on the proxy servers and how optimized the polling scheduler is, there may be delays between the NMS's polling of a proxy server and the return of information about the members of the proxy server's group.

The need to establish groups and proxy servers dynamically, distribute polling responsibilities among proxy servers, and optimally schedule polling makes this strategy com-

plex. This violates the general systems design principle is to keep things as simple as possible [14].

Both the NMS's client polling program and the SNMP agent in the mobile hosts need to be modified to support this new strategy. The mobile hosts' software needs to be changed to support grouping, polling of group members, and proxy serving of accumulated group network management information. The NMS's client polling mechanism must be modified to support affiliations with proxy servers and polling to gather group information.

5.5.3 Evaluation

Although the bandwidth reductions of the SNMP proxy server strategy are significantly greater than that of the other two alternative strategies, the necessary software modifications on both the NMS and the mobile hosts are substantially more than the other strategies. While the other relatively simple strategies rely on time tested SNMP tools, the SNMP proxy strategy has the added complexity of requiring new mechanisms and algorithms to achieve efficiency.

For BBN, the added benefit of the SNMP proxy server mechanism being easily adapted into a clustered mobile wireless ad hoc network makes this strategy attractive.

5.6 Using OSPF routing updates to do network management

The bandwidth required to support SNMP response traffic using the OSPF strategy is (from Table 4.5):

$$\text{OSPF SNMP Response Traffic}_{max} = (N-1) \cdot 11.34 \text{ bps} \tag{5.12}$$

To support this network management traffic, link rates need to be:

$$\text{Link rate} = (N-1) \cdot 11.34 \text{ bps} \cdot 20 = 226.8 \cdot (N-1) \text{ bps} \tag{5.13}$$

With BBN's mobile wireless network's 50 kbps links in each direction, we can support 221 mobile hosts (531% gain over standard SNMP polling):

$$N = \frac{50000 \text{ bps}}{226.8} + 1 \approx 221 \text{ mobile hosts} \tag{5.14}$$

5.6.1 Advantages

The OSPF strategy of listening to routing updates to ascertain network management information eliminates network management traffic for high priority fault and topology detection. This significantly lowers network management bandwidth usage, and allows the management of more than five times as many mobile hosts as standard SNMP polling.

Only network management data gathering client needs to be changed - not SNMP agents. Hence, the mobile hosts' software does not have to be modified to reflect any changes.

5.6.2 Disadvantages

Unlike the adaptive SNMP polling algorithm, this OSPF network management strategy is not a simple modification of the network management station's polling client. To implement the OSPF strategy, an entirely new client that understands OSPF and can masquerade as a mobile host running the OSPF algorithm needs to be developed. This client must then keep track of the topology and status of the network, and filter relevant information back to the network management station. BBN's mobile hosts are already running the OSPF routing protocol, so only the client on the network management station needs to be modified.

This OSPF strategy is dependent on the routing protocol. If there is a future change in the routing protocol, the entire network management solution may need to be modified or replaced.

5.6.3 Evaluation

The OSPF strategy provides a viable solution for constraining bandwidth usage for network mangement over mobile wireless networks that are currently running OSPF (or a variant of it that also uses link state updates). A large percentage of the network management response traffic (84.2%) is replaced by routing overhead that is already on the network allowing more than five times as many mobile hosts to be managed as standard SNMP polling.

This solution, however, still leaves a considerable amount of low priority and performance management traffic on the network. Also, there are significant software developement costs associated with implementing this strategy. Finally, by breaking an abstraction barrier and having the higher level network management layer dependent on the lower level routing layer for network management updates, this strategy imposes a dependency on the OSPF routing protocol (if the routing protocol changes, the network management strategy may have to change too).

5.7 Summary

A graphical representation of the link rate required for each network management strategy as a function of the number of nodes is given below.

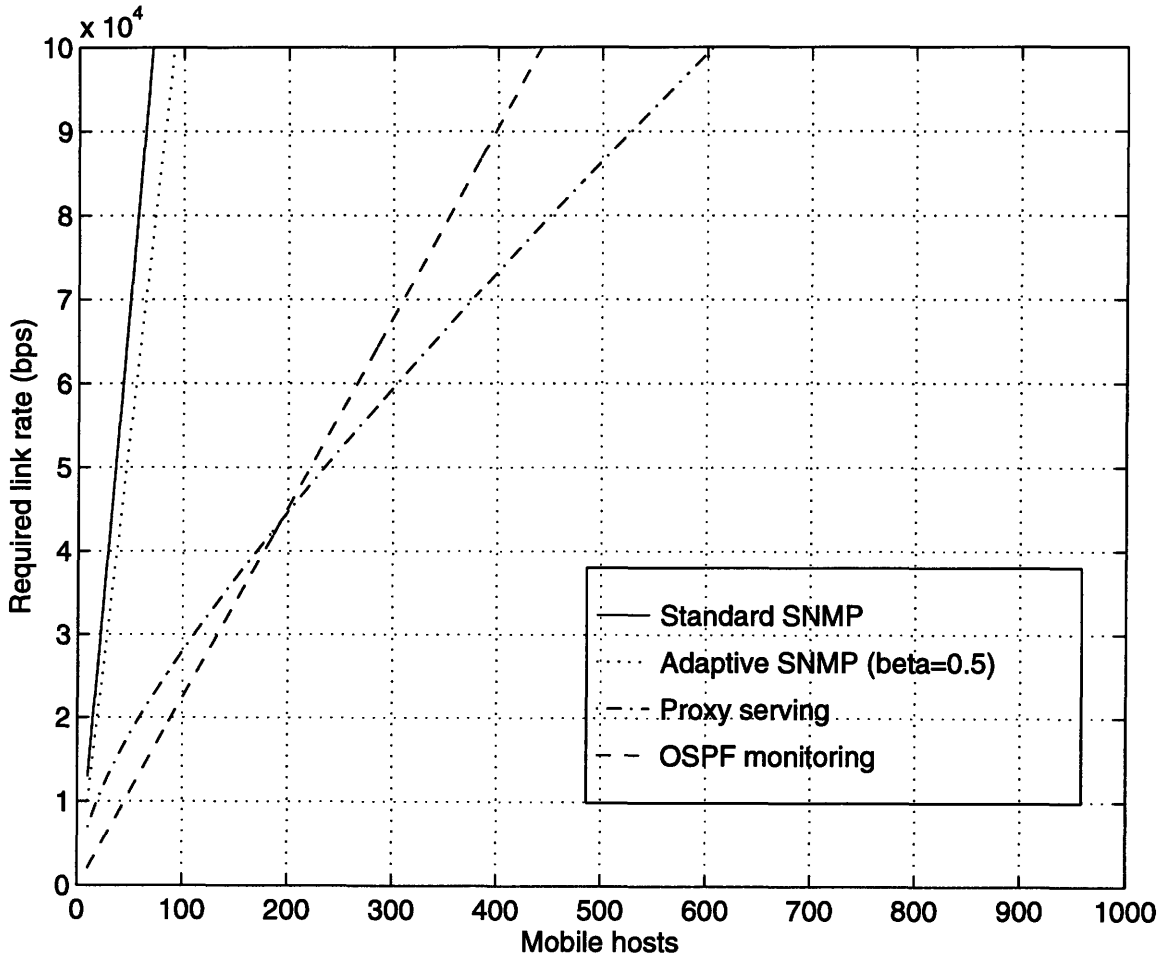

Figure 5.1: Graph of worse case required link rates for four network management strategies

As seen from Figure 5.1, for BBN networks with link rates of 50 kbps, the proxy server strategy allows the most mobile hosts to be monitored (248 mobile hosts), with OSPF monitoring strategy following closely behind (221 mobile hosts). Standard SNMP polling and adaptive SNMP polling allow an order of magnitude lower number of hosts to be monitored (35, and 35-64 mobile hosts as β varies from 0 to 1, respectively).

For the prescribed polling intervals and information required, none of these network management strategies can provide adequate service for mobile wireless networks that are greater than 224 nodes. It is important to note, however, that these values are derived assuming the worse case completely elongated network topology (a 1xN network), where all the polls have to go through one link. The number of mobile hosts that can be polled increases linearly with respect to the number of links connected the NMS's mobile host (in the case of the proxy server network management strategy, also the number of links connecting the proxy server to its group). For example, a completely uniform distribution with two links extending from the NMS's mobile host will double the number of mobile hosts that can be polled for each strategy.

If the network management station were placed in the center of the mobile wireless network, the maximum number of mobile hosts that could be monitored by the SNMP proxy server strategy becomes 992. Likewise, the number of mobile hosts that can be monitored by standard SNMP, adaptive SNMP (assuming β=0.5), and the OSPF strategy are 140, 184, and 896, respectively. A more reasonable location for the NMS might be at an edge of the mobile wireless network. In the best case, the network management traffic would then be distributed evenly throughout three links, allowing for the management of 744 mobile hosts with the proxy server SNMP strategy, and the OSPF strategy would allow for the monitoring of 663 mobile hosts.

Chapter 6

Conclusion

Standard SNMP polling consumes substantial bandwidth on mobile wireless networks. Using BBN's network model and problem statement, we find that it can support network management for small networks of less than 50 mobile hosts. Adaptive SNMP polling provides mobility dependent optimizations, but still only provides network management capabilities for approximately 50 mobile hosts.

Although SNMP proxy serving and OSPF based network management strategies introduce other disadvantages (e.g. higher implementation costs and network layer compromising), they allow many more mobile hosts to be managed in BBN's mobile wireless network (in the worse case, 248 mobile hosts for SNMP proxy serving, and 221 mobile hosts for the OSPF strategy).

Using BBN's information requirements and network model, none of these solutions allow for the managment of more than 224 mobile hosts. This number can be increased if we move the network management station from the worse case position (in the corner of the network) to any position where it has more links connecting it to the rest of the network (on the side or in the center).

References

[1] D. Johnson, D. Maltz, "Protocols For Adaptive Wireless and Mobile Networking," *IEEE Personal Communications*, February 1996.

[2] J. Case, M. Fedor, M. Schoffstall, J. Davin, "A Simple Network Management Protocol (SNMP)," RFC 1157, May 1990.

[3] J. Postel, "Internet Control Message Protocol - DARPA Internet Program Protocol Specification," RFC 792, USC/Information Sciences Institute, September 1981.

[4] Stallings, William, *SNMP, SNMPv2, and CMIP*, Don Mills: Addison-Wesley, 1993.

[5] Conversation with Anthony Michel, BBN.

[6] R. E. Kahn, S. Gronemeyer, J. Burchfield, and R. Kunzelman, "Advances in Packet Radio Technology," *Proceedings of the IEEE,* Vol. 66, No. 11, November 1978, pp. 1468-1496.

[7] R. LaMaire, A. Krishna, P. Bhagwat, and J. Panian, "Wireless LANs and Mobile Networking: Standards and Future Directions," *IEEE Personal Communications*, August 1996.

[8] S.M. Dauber, "Finding Fault," *Byte*, March 1991, pp. 207-214.

[9] Mobile MIB Task Force, "Mobile MIB Draft mibs," http://www.epilogue.com/mmtf/mmtf.html.

[10] R. Aronoff et al, "Network Management Functional Requirements," *NIST Special Publication 500-175, Management of Networks Based on Open Systems Interconnection (OSI): Functional Requirements and Analysis*, Nov. 1989, pp. 24-52.

[11] Comer, Douglas, *Internetworking with TCP/IP Vol. 1, 3rd ed.*, Prentice Hall, Upper Saddle River, NJ, 1995.

[12] Conversation with Mitchell Tasman, BBN.

[13] H. Takagi, *Analysis of Pollying Systems*, MIT Press, Cambridge, MA, 1986.

[14] B. W. Lampson, "Hints for Computer Systems Design," *Proceedings of the Ninth ACM Symposium on Operating Systems Principles,* Bretton Woods, New Hampshire (October 10-13, 1983), pages 33-48.

5000 - 33